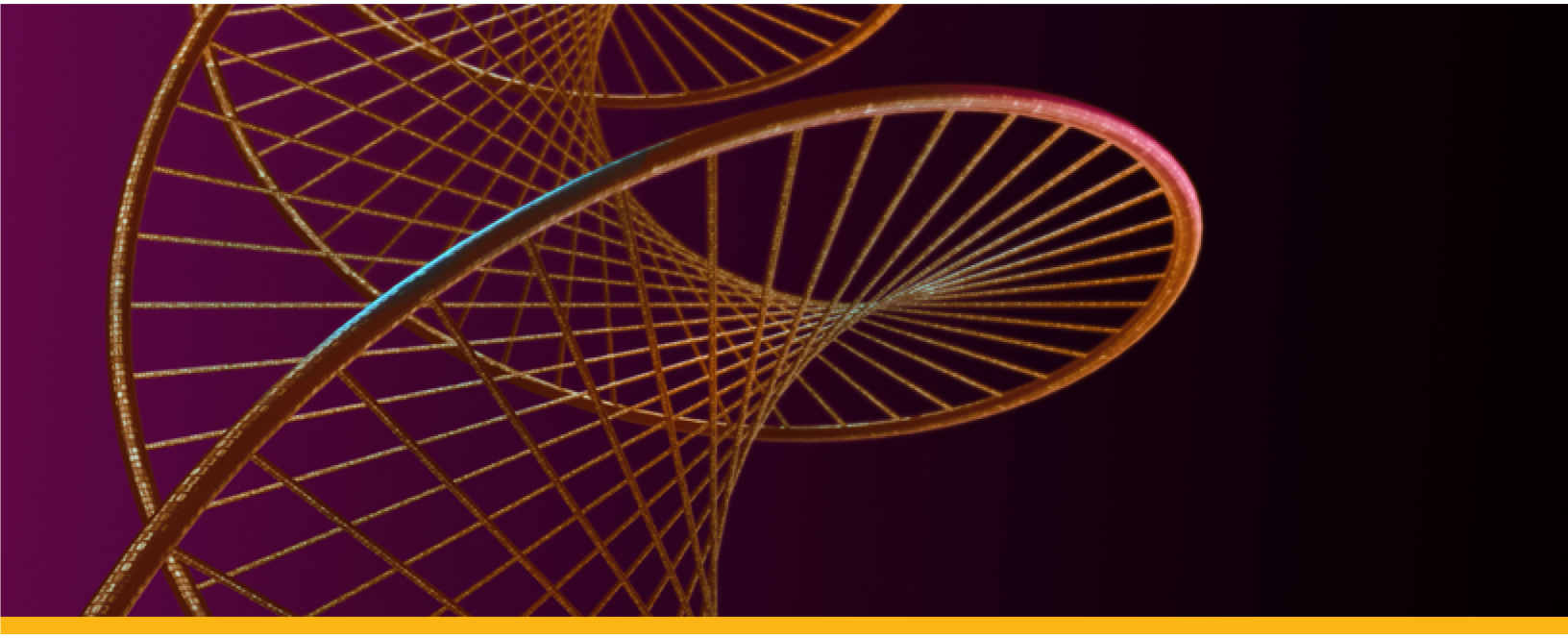
Venafi Trust Protection Platform 25.1

Administration Guide



Venafi
A CyberArk Company

Legal Notices

Copyright © 2007 - 2025 Venafi, Inc and CyberArk Inc. All rights reserved. Covered by United States Patent #7,568,095, #7,650,496, #7,650,497, #7,653,810, #7,698,549, #7,937,583 and other patents pending.

This manual and the software described herein, and the intellectual property rights therein and thereto, are the property of CyberArk, Inc and Venafi Inc. and contain text, data, code, images, graphics, and other information and material that are protected by state, national, and international law pertaining to copyrights, trademarks, patents, trade secrets, and other proprietary rights. CyberArk reserves all rights thereto not expressly granted, including, without limitation, all rights to license, copy, display, distribute, transmit, modify, remove, and create derivative works. The contents of this manual may not be copied or republished without CyberArk's express written permission. The software described in this manual may only be accessed and used pursuant to a valid current license agreement, and in compliance with our End User License Agreement (docs.venafi.com/r/eula) under which licensees are prohibited from distributing, copying, or sharing the licensed software for any purpose other than internal use by licensee for bona fide machine identity management services and compliance monitoring.

"Venafi" and "CyberArk " are registered trademarks of CyberArk Inc in the United States and many other countries, and may be pending trademarks in other countries. The Venafi logo, the CyberArk logo, "Control Plane for Machine Identities," "Trust Protection Platform," VIA Venafi, Venafi TLS Protect for Kubernetes, and other CyberArk group entity names and product names are trademarks of CyberArk, Inc. in the United States and other countries. Other company, product names, and trademarks mentioned in this document are the property of their respective owners. The use of the word "partner" does not imply a Partnership Relationship between CyberArk and any other company.

Online Documentation

This manual and other Venafi documentation are available at the Venafi Documentation Portal at https://docs.venafi.com/25.1.

Feedback - We love hearing from you

We welcome your feedback on our documentation. If you have something you'd like to share, or a way we could improve, please send the following information to documentationfeedback@venafi.com: [1] The name of the PDF guide (Administration Guide); [2] The version of Venafi Platform you are using (25.1); [3] Your feedback.

Venafi Corporate Office

Address: 175 E 400 South, Suite 300
Salt Lake City, UT 84111
USA

Phone: 801-676-6900

URL: https://www.venafi.com/

Venafi Customer Support

Phone: 877-266-5159

Email: support@venafi.com

URL: https://community.cyberark.com

Released: June 2025. Document Version Number: 25.1.0

Chapter 1: VIA Venafi and our No Outage Guarantee 23

About this guide 1

Chapter 2: About Venafi Trust Protection Platform administration consoles 3

Customer Experience Improvement Project 4

Unified menu bar and SSO 5

Responsive layout 6

Customizing the product menus 6

Working with the User Menu 7

My Account 8

My Teams 9

Approvals 10

Preferences 11

About menu - Viewing system information 14

Working with the web consoles 14

Customizing the look of the login screen 15

About the Venafi CodeSign Protect web interface 17

Working with the Policy Tree 17

Logging in 17

Navigating the Policy tree 18

Reports tab 19

Using the Policy Tree's tree view 19

Using the Policy Tree's view buttons 22

About the Policy Tree's detail view ... 23
Policy Tree's detail view buttons ... 23
Adding objects to the policy tree ... 28
Deleting objects ... 31
Moving objects ... 33
Renaming objects ... 36
Filtering the Tree view ... 37
Searching the policy tree ... 38
Start the console in Query mode ... 41
Finding objects in the Policy tree ... 42
Venafi Configuration Console ... 44
Answer File wizard ... 46
Configuring allowed algorithms ... 56
Attention Required ... 56
Database configuration ... 58
Product configuration ... 64
Connectors configuration ... 76
System Roles ... 109
Authentication configuration ... 109
Venafi Recycle Bin ... 138
Access Management ... 153
Code Signing ... 170
Events ... 254
Statistics ... 254
Venafi Message Bus ... 255
Tools ... 263

Chapter 3: Log server ... 265

Chapter 4: Default channel 266

Chapter 5: Event definitions for server components 266

Chapter 6: Logging tree 268

Venafi Configuration Console or the Tools MMC Snap-in? 268

Event definitions VCC Node 269

Channels VCC Node 269

Notification Rules VCC Node 270

Servers VCC Node 270

Information about multiple log servers 270

Chapter 7: Log events 271

Chapter 8: Event IDs and severity levels 271

Chapter 9: Customizing event definitions 272

Resetting to original event definitions 273

Chapter 10: Creating custom logging event definitions 273

Chapter 11: SQL Server channel requirements 290

Chapter 12: SQL Server channel configuration 291

Chapter 13: Updating the SQL Server channel object 294

Chapter 14: Creating a SQL Server log channel 294

Chapter 15: SMTP channel factory template upgrade considerations 297

Chapter 16: SMTP outbound server configuration 297

Chapter 17: Email templates 298
Email Templates in VCC 298
Customization and Upgrades 299
Flexibility in Configuration 299
Chapter 18: Managing logos and images used in email templates 299
Chapter 19: About SMTP templates for email notifications 302
Where to Find Templates 302
Customizing Templates 302
Setting the Default Template 302
Preservation During Upgrades 303
Resetting to Default Configuration 303
Chapter 20: Editing SMTP message templates 303
Using the Template Editor 304
Working with macros, images, and variables 304
Macros 304
Images 304
Variables 304
HTML and plain text messages 305
Saving your changes 306
Chapter 21: Built-in SMTP channels 306
SMTP channel properties 307
Chapter 22: Editing SMTP channel message contents for email notifications 311
Specify a template 311
Preview the message 311
Define variable values 311

Using macros in the SMTP Message Editor 312

Chapter 23: Message delivery failures 312

Chapter 24: Adaptable Log Channel prerequisites 313

What's next? 314

Chapter 25: About the Adaptable Log Channel PowerShell script 314

Chapter 26: Example: creating a ServiceNow incident for expiring certificates 317

Chapter 27: Configuring the Adaptable Log Channel object 318

Chapter 28: Protecting against unapproved changes to Adaptable Log Channel scripts 321

Chapter 29: PowerShell script reference for Adaptable Log Channel 322

About debug logging 323

Chapter 30: About hash tables 324

Chapter 31: Perform-Action function 324

How it works 325

Chapter 32: File channel requirements 329

Chapter 33: File channel configuration 329

Chapter 34: Filter channel configuration 333

What happens if I select items for both Events and Severity? 334

SNMP Versions and Compatibility 334

Management Information Base (MIB) 335

Customizing the MIB 335

Chapter 35: SNMP channel requirements 335

Chapter 36: SNMP Channel object configuration 336

Chapter 37: Customizing the Management Information Base 339

About the CEF format 341

About the JSON format 341

About the BSD format 342

About TLS 342

Chapter 38: Syslog channel prerequisites 342

Chapter 39: To configure a syslog channel object 343

Notification rule editor operators 350

Notification rule variables and supported operators 352

Login failure notification 354

Successful login from unknown IP address notification 354

Showing the correct IP address when using a load balancer to show the correct IP address 355

Automatic credential rotation options 356

Database Connection Repair 359

How to recover a broken HSM connection 360

Venafi MMC Snap-In Collection 361

Install the Venafi MMC Snap-In Collection 363

Venafi CodeSign Protect Administration Snap-In 374

Venafi Event Viewer 374

Venafi Statistics Viewer 384

Venafi Recycle Bin 389

Access Management 389

Venafi Message Bus 407

Tools 416

Chapter 40: Log server 418

Chapter 41: Default channel 418

Chapter 42: Event definitions for server components 419

Chapter 43: Logging tree 421

Venafi Configuration Console or the Tools MMC Snap-in? 421

Event definitions VCC Node 422

Channels VCC Node 422

Notification Rules VCC Node 423

Servers VCC Node 423

Information about multiple log servers 423

Chapter 44: Log events 424

Chapter 45: Event IDs and severity levels 424

Chapter 46: Customizing event definitions 425

Resetting to original event definitions 426

Chapter 47: Creating custom logging event definitions 426

Chapter 48: SQL Server channel requirements 444

Chapter 49: SQL Server channel configuration 445

Chapter 50: Updating the SQL Server channel object 448

Chapter 51: Creating a SQL Server log channel 448

Chapter 52: SMTP channel factory template upgrade considerations 451

Chapter 53: SMTP outbound server configuration 451

Chapter 54: Email templates 452

Email Templates in VCC 452

Customization and Upgrades 453

Flexibility in Configuration 453

Chapter 55: Managing logos and images used in email templates 453

Chapter 56: About SMTP templates for email notifications 456

Where to Find Templates 456

Customizing Templates 456

Setting the Default Template 456

Preservation During Upgrades 457

Resetting to Default Configuration 457

Chapter 57: Editing SMTP message templates 457

Using the Template Editor 458

Working with macros, images, and variables 458

Macros 458

Images 458

Variables 458

HTML and plain text messages 459

Saving your changes 460

Chapter 58: Built-in SMTP channels 460

SMTP channel properties 461

Chapter 59: Editing SMTP channel message contents for email notifications 465

Specify a template 465

Preview the message 465

Define variable values 465
Using macros in the SMTP Message Editor 466
Chapter 60: Message delivery failures 466
Chapter 61: Adaptable Log Channel prerequisites 467
What's next? 468
Chapter 62: About the Adaptable Log Channel PowerShell script 468
Chapter 63: Example: creating a ServiceNow incident for expiring certificates 471
Chapter 64: Configuring the Adaptable Log Channel object 472
Chapter 65: Protecting against unapproved changes to Adaptable Log Channel scripts 475
Chapter 66: PowerShell script reference for Adaptable Log Channel 476
About debug logging 477
Chapter 67: About hash tables 478
Chapter 68: Perform-Action function 478
How it works 479
Chapter 69: File channel requirements 483
Chapter 70: File channel configuration 483
Chapter 71: Filter channel configuration 487
What happens if I select items for both Events and Severity? 488
SNMP Versions and Compatibility 488
Management Information Base (MIB) 489

Customizing the MIB 489

Chapter 72: SNMP channel requirements 489

Chapter 73: SNMP Channel object configuration 490

Chapter 74: Customizing the Management Information Base 493

About the CEF format 495

About the JSON format 495

About the BSD format 496

About TLS 496

Chapter 75: Syslog channel prerequisites 496

Chapter 76: To configure a syslog channel object 497

Notification rule editor operators 504

Notification rule variables and supported operators 505

Login failure notification 507

Successful login from unknown IP address notification 507

Showing the correct IP address when using a load balancer to show the correct IP address 508

Working with Venafi Platform 509

Using the TppConfiguration command line tool 511

TPPConfiguration syntax 513

Configuration switches for TppConfiguration.exe command line tool 514

Using TppTool from the command line and script files 519

TppTool syntax 520

TppTool parameters and options 521

Using the TppPKIs command line tool 524

TPPPKIs tool syntax 524

Examples 528

Chapter 77: Trust Protection Platform configuration overview 531
General configuration options 534
Securing Trust Protection Platform's web servers 535
Exceptions to HTTPS Redirects 536
About the Venafi Operational Certificate 536
Replacing the Venafi Operational Certificate (VOC) with your own CA-signed certificate 536
Troubleshooting: manually enabling HTTPS 537
Supported SSH Ciphers, HMACs, Key Exchanges, and Public Keys 540
Common Criteria Compliance 542
Error scenario 543
Chapter 78: Managing system encryption keys 545
Overview of encryption drivers 546
Configuring the root encryption driver 549
Database Encryption 551
Software Encryption 551
Hardware Encryption 552
Tips for using both types of encryption 552
Adding software encryption to an existing system 552
Managing the default software encryption key 553
Backing up the software encryption key 554
Managing the null key 555
Using HSM-protected encryption keys 557
What's next? 558
HSM Configuration 558
AWS CloudHSM configuration requirements 561
Creating a HSM connector 562

Enabling HSM connection debugging ... 564
Validating encryption keys ... 566
Using encryption keys to secure encryption assets ... 566
Understanding cryptographic algorithms in Venafi Trust Protection Platform ... 566
Algorithm types supported by Venafi Platform ... 572
About default algorithm configuration ... 573
Configuring allowed algorithms ... 574
Managing encryption keys in the Policy tree ... 575
Managing encryption keys in the Credentials Tree ... 577
Rotating encryption keys for a policy or ObjectDN ... 578
Venafi Advanced Key Protect ... 580
Central private key generation ... 580
Remote private key generation ... 581
Supported methods of key generation ... 581
Managing applications using HSM-protected keys and Venafi Advanced Key Protect ... 588
Enabling Venafi Advanced Key Protect ... 590
Enabling remote key generation for Apache certificates ... 590
Enabling remote key generation for CAPI certificates ... 593
Enabling remote key generation for JKS certificates ... 594

Chapter 79: Using the dashboards ... 597
About Dashboard widgets ... 599
Working with the All Certificates (dashboard) ... 599
Certificate Authorities widget ... 600
Certificate Expiration widget ... 600
Certificate Key Size widget ... 600
Certificate Protection Level widget ... 601
Certificate Signing Algorithm Widget ... 601

Certificate Totals widget 602
Certificate Trends widget 605
Certificate Validity Period widget 607
Chain Validation widget 607
End Entity Validation widget 608
Secure Protocols vs Insecure Protocols widget 609
Working with the User and Client Device Certificate (dashboard) 610
Client Certificate Totals Widget 610
Certificate Key Size widget 614
Certificate Signing Algorithm Widget 614
Certificate Protection Level widget 615
Certificate Validity Period widget 615
Certificate Authorities widget 615
Certificate Expiration widget 616
Certificate Origin widget 616
Certificate Trends widget 616
Working with the SSH Keys (dashboard) 618
Key Totals widget 618
SSH key algorithm widget 620
Key Size widget 621
Network Discovery–Key Size widget 622
SSH Network Discovery Summary widget 623
Trust distribution per User widget 626
SSH trends widget 627
Working with the System Status (dashboard) 629
License Counts 629
Engine Connections 630

Configuring value thresholds using Account Preferences 631
TLS Protect and Client Protect settings 632
SSH Protect settings 633
CodeSign Protect settings 633

Chapter 80: Working with identities, permissions, and teams 635
Managing identities from third-party data providers 636
Working with Active Directory 636
Working with LDAP and Oracle directory service 648
Automatic configuration of domain controllers and global catalogs 672
Allowing AD and LDAP users to see teams and local users 672
Creating and managing teams 673
Setting team policies and permissions 674
Allowing AD and LDAP users to see teams and local users 688
Working with teams 689
Join a team 692
Managing local identities directly in Trust Protection Platform 693
A note about identity security across multiple directories 693
Managing the Local user directory 694
Configuring the Local connection 694
Creating local user identities 696
Specifying who should get default system notifications 697
Local user configuration settings 698
Changing local user passwords 700
Revoking a user's access grant 700
Creating Local groups and teams 702
Editing teams 705
Deleting teams 706

Understanding system roles 706
About the Master Admin role 708
Managing system role assignments in Venafi Configuration Console 709
Managing role and grant assignments in Policy Tree 710
About viewing users that have the Master Admin role in Aperture 711
About API Default Settings 712
Managing permissions for identities 713
Permissions overview 713
User permissions 713
Viewing user entitlements 714
About Permissions and Inheritance 716
Filtering identities 740
Defining search expressions for AD user directories 740
Filtering user directories in Policy Tree 744
Modifying TLS Protect user and group permissions 745
Filtering by users, teams, or roles using the Identity Inventory 746
Viewing identity details 747
Updating an identity provider connection password 748
About API integrations 750
Who does what? 751
Integrating other systems with Venafi products 752
API Integrations inventory 756
Updating integration registrations 758
Revoking user and integration grants 760
Deleting API integrations 760
Exporting an API integration 761
Creating, saving, and modifying inventory filters 761

API default settings for remote access configuration ... 763

Chapter 81: Configuring the Venafi Trust Protection Platform server object ... 767

Configuring the Trust Protection Platform server ... 768

Trust Protection Platform server configuration ... 768

About using an HTTP proxy ... 784

Configuring an HTTP proxy ... 787

Chapter 82: Alternate authentication and login options (including single sign-on) ... 791

Setting up certificate authentication for web console ... 793

Setting up certificate authentication for API remote access ... 794

About Integrated MS Windows Authentication ... 796

Setting up Windows Integrated Authentication for the web console ... 797

Enabling RSA SecurID ... 802

Oracle Access Manager settings ... 809

Prerequisites for Configuration ... 809

System requirements for Oracle Access Manager ... 810

Working with SAML for single sign-on (SSO) ... 810

Configuration process ... 811

Technical implementation details ... 812

Prepare Venafi Platform for SAML SSO ... 813

How to configure ADFS for SSO ... 819

How to configure Azure for SSO ... 822

How to configure Okta for SSO ... 824

How to configure PingFederate for SSO ... 826

How to configure PingOne for Enterprise for SSO ... 831

Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML ... 834

SAML troubleshooting tips ... 835

Chapter 83: Setting up Certificate Verification for securing outbound HTTPS connections 839

Chapter 84: Trust Protection Platform components 843

Configuring the Validation Manager module 851

Configuring the Reporting module 852

Configuring the Monitor module 854

Configuring the Discovery module 855

Chapter 85: Using policies to manage encryption assets 859

How policies work 860

How policies work at the object level 860

How policies work at the value level 861

Locking policy values 863

Locking and unlocking policy values 863

Policy structure examples 865

Management level 866

Organizational Folder Structure 867

Overview of certificate types 868

Using multiple structures 872

Managing your policies (folders) 874

About policy (folder) hierarchies 874

Creating policies 874

Configuring policies 878

Configuring a policy's subordinate objects 888

Chapter 86: Working with custom fields 891

Adding or deleting a custom field 893

Custom field configuration settings ... 894
Creating a single or multi-select list in a custom field ... 897
Editing a custom field ... 900
Filtering custom fields ... 901
Viewing custom fields ... 902
Generating a Custom Fields report ... 903
Using the Custom Field macro for notifications ... 905
Basic macro ... 905
Macro for multiple stored values ... 906
Macro for making a multi-select list human readable ... 907

Chapter 87: Working with system credentials ... 909
About credential object hierarchy ... 911
About securing credential objects ... 911
About credential objects ... 912
Creating new credentials ... 912
Creating user name or password credentials ... 913
Creating private key credentials ... 916
Creating certificate credentials ... 918
Creating Amazon credentials ... 919
Creating Adaptable Credentials ... 921
About generic credential object configuration settings ... 925
Creating credentials using Policy Tree ... 927
Managing existing credentials ... 929
Filter Panel Types ... 931
Exploring credential details ... 933
Viewing how a credential is being used ... 936
Exploring permissions assigned to a credential ... 937

Editing credentials 937
Replacing a private key credential's private key 938
Moving a credential to another folder 939
Deleting credentials 940
About Amazon credentials 940
Authorizing the use of EC2 Assigned Role for Amazon credentials 941
Authenticating to multiple AWS accounts using a single Amazon Credential 942
Using CyberArk with Trust Protection Platform 944
Getting CyberArk ready for integration with Trust Protection Platform 944
About securing a CyberArk application 948
Creating a CyberArk Application for TPP 948
Creating a CyberArk connector 951
Configuring and editing the CyberArk Credentials driver in the Policy Tree 956
Adding and configuring CyberArk credentials 958
Editing the CyberArk Web Service credential 959
Granting access to CyberArk Application Identity Manager (AIM) 960
CyberArk user and password integration requirements 963
Using a CyberArk credential for provisioning (certificate installation) 964
Check CyberArk permissions on safe members 965
PowerShell script reference for Adaptable Credential 966
About hash tables for Adaptable Credentials 968
Adding custom fields to your Adaptable Credential 968
Test-Connector function 970
Retrieve-Credential function 971
Protecting against unapproved changes to Adaptable Credential scripts 972
About Generational Management 974

Chapter 88: Venafi Trust Protection Platform reports 975
Managing system reports 977
About reports 977
Configuring the root report object 978
Creating reports in the Policy Tree 979
Manually generating reports 980
Chapter 89: Understanding system logging and notifications 983
Logging system overview 983
Log events 984
Appendix A: Enabling Demo Mode 985
Appendix B: Venafi Data Privacy Policy for Venafi Trust Protection Platform™ 987
Types of information we collect 987
Your installation of Venafi Trust Protection Platform 987
How we use the information we collect 988
Provide our services 988
Maintain & improve our services 988
Measure performance 988
How we use cookies in our products 988
What is a Cookie? 988
What Cookies does Venafi use? 989
How long we store the information we collect 989
Appendix C: Open Source Information 991

VIA Venafi and our No Outage Guarantee

Certificate outages can be debilitating for critical security and operational systems in your organization. They can result in down systems, lost sales, and the inability for customers to use your services.

Venafi has created a specific, comprehensive, and proven path that, when followed, guarantees you will stop certificate outages before they occur. This path encompasses the people, the processes, and the technologies that eliminates outages.

VIA Venafi is a combination of technology, experience, and proven expertise that helps drive you to common goals. Focused on Venafi technology that delivers the Visibility, Intelligence, and Automation to protect machine identities of all types, this approach is based on access to and a deep understanding of all the needed components.

If you have an outage that directly results from an expired or mis-configured certificate in the Venafi Platform, and that certificate was configured and protected in a manner compliant with the Venafi Way, we will make it right by providing at no charge to you Venafi subject matter experts to help investigate the failure, perform a root cause analysis, and specify the actions needed to remediate and avoid recurrence of that same problem.

To assist you in understanding where you and your organization is along the VIA Venafi path, we offer a free VIA Venafi Review. As a Venafi customer, you can request a progress assessment from Venafi experts at no cost.

The 8 critical steps of the VIA Venafi Proven Path are:

1. Establish and outage safety Network Appliance
2. Establish a foundation for the outage prevention solution
3. Align the organization around a service-based approach
4. Define and design the services
5. Train the teams who support the services, and document the processes

6. Recruit, train, and onboard early adoption teams for initial rollout
7. Expand adoption: onboard certificate owners for enterprise rollout
8. Assess service effectiveness, tune, and evaluate the adoption process

For additional information about the VIA Venafi Proven Path, a free VIA Venafi Review, and the VIA Venafi No Outage Guarantee, please contact Venafi customer support.

About this guide

Venafi Trust Protection Platform™ automates the provisioning, discovery, monitoring, validation and management of encryption keys and digital certificates. Trust Protection Platform supports heterogeneous certificate authorities (CAs), multiple platform deployments, and various encryption types, and has proven scalability within some of the world's largest deployments. With Trust Protection Platform, you can ensure that your encryption systems provide the security they are designed to deliver while at the same time reducing operational risk and administrative workload.

In this context, Venafi Platform refers to the collective set of tools and common components used to power Venafi TLS Protect, Venafi SSH Protect, Venafi Client Protect, and Venafi CodeSign Protect.

You will use the Platform to install Venafi products, configure servers and services, and upgrade to newer versions of Venafi software.

Venafi Platform settings and configuration are accessed by a system administrator or a server administrator. The administrator may be interested in the following tasks:

- System requirements for Venafi components
- Preparing your environment for the Venafi Platform
- Installing Trust Protection Platform
- Command line installation and configuration
- Upgrading to the 25.1 quarterly release
- Updating the latest patch
- About rolling upgrades
- Disaster recovery operations

For information about the Platform menu, see "Working with Venafi Platform" on page 509.

1

About Venafi Trust Protection Platform administration consoles

Venafi Trust Protection Platform™ provides two consoles:

- A web-based console that can be launched by connecting to the Venafi server using a browser. This web console provides two experiences (during our multi-year effort to unify into a single modern console):
    - OneVenafi - this is the modernized experience that used to be called Aperture. Most activities (including non-admin activities) are part of this experience.
    - Policy Tree - this is the classic experience that used to be called WebAdmin. This experience is gradually being retired as features are moved to the OneVenafi experience. Most of the features in this experience are configuration and administrative activities.
- Venafi Configuration Console (VCC): A powerful MMC snap-in console that allows you to administer the settings of the Venafi Platform installation, as well as work with CodeSign Protect and the Venafi Event Viewer. VCC allows you to control Venafi services, enable product components, configure database settings, update email notifications, control identity access including LDAP, AD, and SSO.

Customer Experience Improvement Project

When you install Venafi Trust Protection Platform, certain telemetry data is collected. This information is used for license compliance, and allows us to collect non-personally identifiable information about how you use the product. In return, you receive push notifications of important events (like software upgrade availability), as well as enhanced in-product help. Venafi uses the data collected through this feature to make product road map decisions.

For more information see the "Venafi Data Privacy Policy for Venafi Trust Protection Platform™" on page 987.

To see the list of supported browsers, see System requirements for Venafi components.

This chapter contains the following topics:

Unified menu bar and SSO

We're building towards a single, unified administration console. In versions prior to 21.2, you might switch between the Aperture and WebAdmin consoles to perform different functions. You used the Product Switcher to move between consoles with single sign-on (SSO) keeping you in logged in to both.

Starting in 21.2, the Product Switcher allows you to select between installed Venafi products (e.g. TLS Protect, SSH Protect, etc.). Depending on the menu item you click, you will be directed to the correct interface. Each product has its own custom menu that helps you with the tasks related to that product.

If you've been using a version of Venafi Platform older than 21.2, you may need to make some adjustments based on these new menus. For example, the menus can be customized by both users and system administrators.

If you are looking for the features that were in the console we called **WebAdmin**, look for the **Policy Tree** menu item, which is where these features continue to live while they are being moved to the individual products.

When working with the menus, be aware of the following:

A. Click any of the menu items to access sub-menus.

   If you don't see a menu or sub-menu item, it's because your user account doesn't have access to items, or because your administrator has turned off that menu item by default. (For more information about custom menus, see "Customizing product menus" on page 13.)

   For example, in TLS Protect, you only see the Certificate Inventory if you have *read* or *view* access to certificates.

B. Type the first few characters of any asset in the **Global Search** to get an automatic preview of results. If there are more than a few results, the *Show All Results* option lets you see all discovered items in a list view.

C. To switch between products use the Product Switcher.

   What you see on the Product Switcher depends on your user account and which products you have licensed and installed. For example, master administrators see TLS Protect and Platform; Other products that are part of the suite, but are not licensed are shown in the Product Switcher with "Learn More" links, allowing you to learn more about other products that can enhance your machine identity protection processes.

D. When you're on the Dashboards page, click the dots below the menu bar to navigate between dashboards.

E. A responsive layout lets you resize the browser window to collapse the menu bar.

Responsive layout

A responsive layout lets you resize the browser window to collapse the menu bar. When you click it, you have access to all of the options available in the menu bar, user menu, and Help Library.

Customizing the product menus

As a user, you can customize the menus to only show the features you use for supported products. If you are a master administrator, you have the ability to set the default menus a user sees when they log in.

This is not a security feature. It is a convenience feature to make the product easier to use, however it does nothing to restrict users from accessing any features in the product if they enter the correct URLs. In addition, even if an admin turns off a menu item for users, **any user can configure their own settings and override the defaults set by the administrator**.

To customize product menus for your own account

1. From the **Product Switcher** on the top menu, click the product whose menu you want to customize.

   > **TIP** This step is important because the Navigation Menu settings on Preferences only apply to the product you are currently in. You will need to repeat this process for each product whose menu you want to customize.

2. From the **User** menu, click **Preferences**.
3. Click **Navigation Menu**.

   A modal window appears with the **Mine** tab selected.

4. Use the switches to enable (switch on right) or disable (switch on left) menu items.
5. Use the down button to expand a top-level menu.
6. Click the flag icon to set the default landing page (the page you see when you open that product).
7. Click **Save**.

If you changed your default landing page, that setting will take effect the next time you log in.

If you want to go back to the default settings for this product, click **Restore Defaults**.

Repeat these steps for other products, if desired.

To customize default product menus settings for non-admins

1. From the **Product Switcher** on the top menu, click the product whose menu you want to customize.

   > **TIP** This step is important because the Navigation Menu settings on Preferences only apply to the product you are currently in. You will need to repeat this process for each product whose menu you want to customize.

2. From the **User** menu, click **Preferences**.
3. Click **Navigation Menu**.

   A modal window appears with the **Mine** tab selected. This is where you would configure settings for *your own account*.

4. Click **Everyone Else**.
5. Use the switches to enable (switch on right) or disable (switch on left) menu items.
6. Use the down button to expand a top-level menu.
7. Click the flag icon to set the default landing page (the page your users see when they open that product).
8. Click **Save**.

To reset the default settings provided by Venafi for the product, click **Restore Defaults**.

Repeat these steps for other supported products, if desired.

Working with the User Menu

The User Menu is a new feature on the unified menu bar that gives you control over your account preferences, account settings, teams, and approvals. This is also where you go to log out of your Venafi session.

Additional details about each of these features can be found in the following topics:

- "My Account" below
- "My Teams" on the facing page
- "Approvals" on page 10
- "Preferences" on page 11
- "About menu - Viewing system information" on page 14

My Account

The **My Account** link in the User Menu takes you to your identity details page.

My Account displays information about your user account.

Under **Information**, you can see role information about the identity. If your account has the `Master Admin` permission, you will also be able to see some of the roles the user has.

The above settings are `read-only` on the My Account page. To modify them,

1. From the Platform menu bar, click **Policy Tree**.
2. Open the **Identity** tree.
3. Click on the identity, make changes, and save your changes.

In the side navigation you can view:

- **Certificates** – lists the certificates issued to the user and gives details about the name, expiration date, the key strength, and status of the certificate. Using the drop-down menu, you can choose to either download or revoke the certificate.
- **Mobile Agents**– lists all of the mobile agents on which the user certificates are installed. This list can include devices that were used in the past by the user. The Agent's most recent check in time is also displayed.
- **Permissions Granted**– shows all the permissions that are granted to this user, or to a group that the user is part of. If your account has a role that allows you to manage permissions for an object, click the name of the object to view the object's permissions management page. (You won't see this if you don't have the `Master Admin` role.)

Reset Settings and Preferences

You can reset your settings and preferences from My Account by clicking **Reset Settings & Preferences** at the top of the page. This will reset all stored data about your account including column preferences on inventories, all your dashboard widgets and settings, and any other customizations you've made to Trust Protection Platform.

Reset Password

If you are a local user (your user account was not created by an identity integration like LDAP), you can also change your password from My Account.

- Click **Change Password**.

Change Password requires you to enter your current password. As you type in your new password, your entry is validated against the complexity requirements.

> **DID YOU KNOW?** Password validation takes place locally in your browser. Your password is not transmitted to the server until you click **Change Password**.

If you don't see **Change Password** on your My Account page, then your user identity is not a local account, and your password is not managed by Venafi Platform. Contact your organization to learn how to change your password.

My Teams

The My Teams page provides a list of teams you are assigned to, either as the team owner or as a team member.

This is the same list you would see from the Identity inventory if you used the Member filter to search for your account. (For more information see "Filtering by users, teams, or roles using the Identity Inventory" on page 746).

Depending on your permissions, you may have several options from this page.

- **All users** can click a team name to see details about the team.
- **Users with the Create Team permission** can create new teams.

  For more information, see "Working with teams" on page 689

- **Master Administrators** can delete teams, and configure team settings.

  For more information see "Setting team policies and permissions" on page 674.

Approvals

The Approvals screen allows you to see a list of items waiting for your approval.

> **IMPORTANT** Starting in 20.2, new approvals features are being migrated to this new Approvals screen. Eventually, you will be able to see workflow approvals, key approvals, and more from this screen. **For now, however, you can only see team approval requests on this screen.**

Generally, you'll only have a few items waiting to be approved at once, so you will be able to browse through the list of pending approvals fairly quickly. The approvals list contains the following fields:

Field	Description
Approval Type	Tells you what type of approval is being requested. In 25.1, the only type of approval on this screen is Team Approval.
Description	Provides details about who made the request (display name) and any additional information.
Initiated By	Shows the display name of the user who made the request. Click their name to view their profile.
Team	Which team will be affected by the request.
Initiated At	The time the request was created.
Approval Status	The current status of the approval.

To filter the approval list

You may find it easier to locate a specific request by filtering for it.

1. Click your user icon, then click **Approvals**.
2. Use the filters on the left to narrow the displayed list of approvals. The filters are:
   - Approval Type. This will let you restrict by the Approval Type column. (In 25.1, the only type of approval on this screen is Team Member Approval).
   - Initiated at. Use this to select a date range when the approval request was created.

To take action on an approval request

1. Click your user icon, then click **Approvals**.
2. Locate the approval request.
3. Click **Approve / Reject**.
4. [Optional] Provide comments on your action. This is especially useful if you are rejecting the approval request, as your comments will be sent via email to the requester. Adding a comment about your decision can help the requester know what they can do, if anything, to improve their request.
5. Click **Approve** or **Reject**.

Preferences

The Preferences option on the User Menu takes you to your Account Preferences page, where you can configure specific settings, including customizing the product menus (for supported products).

Throughout system, you see information based on thresholds that you create. This helps to ensure you are protecting your key and certificate data in accordance with your organization's policies and objectives. Venafi Platform is designed to give you flexibility in providing warnings based on thresholds you define. These thresholds affect not only the data you see across the dashboards, but also apply to the way keys and certificates are reported to you throughout Venafi Platform.

You can access Preferences from the User menu to configure these thresholds for yourself.

The master admin can lock values to ensure all users in the organization use the same settings.

Setting threshold values for an individual

1. On the menu, click the user icon, then click **Preferences**.
2. From the left, select a product (TLS Protect & Client Protect; SSH Protect; or CodeSign Protect) depending on which settings you with to modify.
3. Modify the threshold values as needed.
4. Click **Save**.

Setting threshold values across the organization

1. Log in as the master admin.
2. On the menu, click on the user icon, then click **Preferences**.
3. From the left, select a product (TLS Protect & Client Protect; SSH Protect; or CodeSign Protect) depending on which settings you with to modify.
4. Modify the threshold values as needed.
5. Click the lock icon  to prevent others in your organization from setting a different personal value. If the value is locked, and you want users to be able to configure this value for themselves, click the unlock icon  .

   > **NOTE** Modifying these values without locking them will only modify them for your account, not for other users in your organization. Locking these values locks the value for all users.

6. Click **Save**.

TLS Protect and Client Protect settings

Name	Default	Description
Flag certificates which use a key algorithm with a strength of	80 (bits)	For some key types, smaller key lengths are less secure, You can choose to flag and report certificates that use shorter key length algorithms. This value is stored in bits.
Flag certificates with a validity period greater than	397 (Days)	Certificates with long validity periods may be more susceptible to being compromised. Set this value in days. (The default is 397 days.)[1]
Weak Signing Algorithm	None	Allows and reports algorithms considered to be less secure or outdated for signing operations.

[1] In version 20.3 and older, the default value was 820 days, however the major browser vendors no longer accept public certificates with a validity period longer than 397 days. If you had a version of Venafi Platform earlier than 20.4 and you *left this value at the default*, upon upgrade to 20.4 (or later) the new default of 397 days will apply. However, if you had customized this value, upon upgrade to 20.4 (or later) your *previous custom value* will be used.

Name	Default	Description
Flag certificates as Expired - Long Term if expired for longer than	30 (Days)	Expired certificates are grouped into two categories: (1) Expired - short term; and (2) Expired - long term. This helps you with analysis and reporting to recognize items that have recently expired so you can take action on them, if necessary. Set this value in days.
Flag certificates as Expiring Soon if expiring in less than	30 (Days)	To give you enough time to take action on a soon-to-expire certificate, the system begins warning you before a certificate will expire. This value controls how early you want to be alerted to expiring certificates. Set this value in days.
Support Large Object Trees	No	Setting to "Yes" will force all users' administration consoles to launch in query mode. See "Start the console in Query mode" on page 41

SSH Protect settings

Name	Default	Description
Flag certificates which use a key algorithm with a strength of	80 (bits)	For some key types, smaller key lengths are less secure, You can choose to flag and report certificates that use shorter key length algorithms. This value is stored in bits.
Flag keys as Unused Authorized Keys if not used for	365 (Days)	SSH Protect tracks authorized key usage. If an authorized key has not been used for a long period of time it may be time to remove the key so it no longer has any access to your systems. This helps protect your system so old keys can't be used to access the system by somebody who is no longer authorized to have access. Set this value in days.

CodeSign Protect settings

On the CodeSign Protect User Preferences, you can re-enable the First Project dialog, as if you are logging into the product for the first time. Click **Clear Setting** to see this dialog again.

Customizing product menus

From the Preferences menu you can customize your product menus. If you are a master admin, you can also customize the default menus for your organization's users.

For information on customizing the product menus, see "Customizing the product menus" on page 6.

About menu - Viewing system information

Detailed system information about Venafi Platform is available to you on the About page, found on the User Menu. This page shows information including active plugins, installed system version, etc. allowing you to quickly see how your system is configured.

View system information

- On the menu, click on the user icon, then click **About**.

The system information is divided into four tabs:

- **Engine & Schema.** This tab displays your database connection, Aperture version, database schema version, and installation date. Additionally, if the database is connected to other Aperture installations, you can see them here.
- **Loaded API Assemblies.** (Visible to system administrators only.) This tab displays a list of API assemblies that are part of your installation, including the source of the assembly and the version of the assembly installed. These assemblies are part of the Aperture version you have installed, and can't be individually loaded or configured.
- **Loaded UI Plugins.** This tab displays a list of UI plugins that are part of your installation, based on the components you have installed. These plugins can't be loaded or configured individually.
- **Upgrade Status.** (Visible to system administrators only.) This tab shows the upgrade status of all the servers in the cluster, showing what each of their upgrade statuses is. For more information, see Upgrade status page.

Working with the web consoles

> **NOTE** Venafi is in the process of a multi-year effort to unify and modernize the server-based management consoles. As part of that effort, the terms *WebAdmin* and *Aperture* are deprecated. Just focus on the feature you need, and we'll take you to the place to do what you need to do. Some of these screens will use the "WebAdmin" look, which is now called *Policy Tree*. Other screens will look like what we used to call *Aperture*. As we continue our integration effort, eventually you'll just have one consistent UI across all of Venafi's server products.

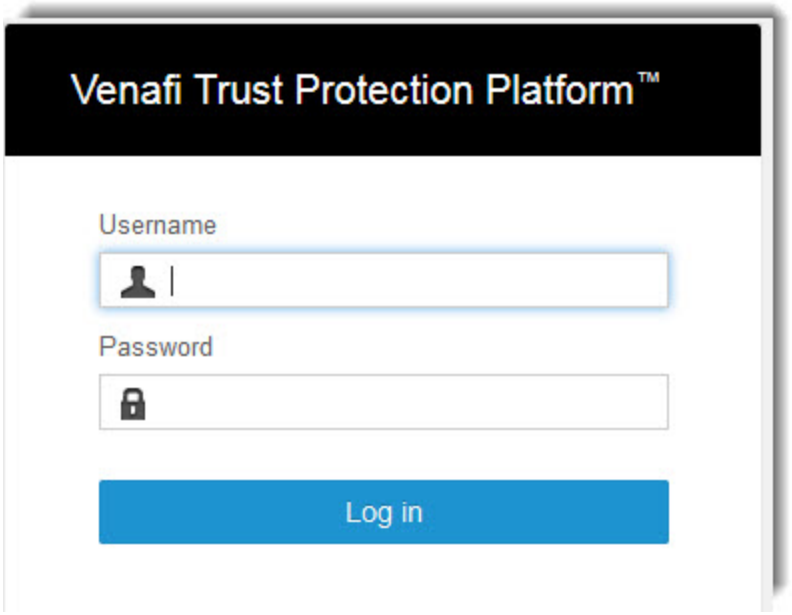
Venafi's web consoles allow you to interact with the Venafi Platform and Venafi products.

In the web console you can:

- Use dashboards to get an overview of the health of your network
- Perform all SSH-related tasks
- Perform all Server Agent tasks
- Perform all certificate tasks

NOTE You must use the Policy Tree to perform advanced certificate tasks such as configuring a CA, creating and configuring applications, and retrying, resetting, or restarting workflows. Reports can only be generated using the Policy Tree. This is easier now using the Product Switcher. See "Unified menu bar and SSO" on page 5 in the Administration Guide.

Customizing the look of the login screen



Venafi Platform lets you customize its labels and styles. Changes to .js and .css files persist across upgrades and patches so customizations do not have to be reapplied.

To customize the look of the Venafi Platform login screen

1. Create a custom terminology file named **terminology-custom-en-us.js**. Customize **label text** using this file.

2. Create a custom style sheet named **terminology-custom-en-us.css**. Customize **styles** using this file.

To download samples of style sheet and terminology files

1. Go to our the articleInfo: Customizing the labels and style of the Aperture Login Page on our Support site and scroll to the bottom of the page. Click the links to download the .zip files
2. Go to our Support site at https://community.cyberark.com/s/article/Info--Customizing-the-labels-and-style-of-the-Aperture-Login-Page. Scroll to the bottom of the page, and then click the links to download the .zip files.
3. Place both files in this location: <*Venafi Home Directory*>:\Program Files\Venafi\Web\Aperture\Client\Plugins\Authorize_Password.
4. (Optional) The first time you add a new terminology file or style sheet to Aperture, IIS must be restarted.

Syntax of the custom terminology file

File must begin with **{** and end with **}**. File must conform to valid JSON syntax. For example, strings that have quotes must be escaped. The syntax of each change of terminology is:

```
"Terminology-Name":"Display Label"
"Username":"Bank E-mail Address"
```

Each line must be separated by a comma. For example:

```
"VenafiTitle": "Bank of Antarctica Certificate Request Portal",
"Username":"Bank E-mail Address"
```

Syntax of the custom style sheet file

A custom style sheet must also have a custom terminology file. Even if the custom terminology file is blank, it must be present in order for Aperture to load a custom stylesheet. The style sheet follows standard CSS3 syntax. For example, This code changes the background color of the header of the login window:

```
#login form .login-header {background-color: #010858}
```

Test Your Changes

If your company decides to apply a customized skin to Aperture, it is strongly recommended that you test your customizations in a non-production environment. Retest your customizations each time you upgrade the Venafi Trust Protection Platform. It is possible that styling classes and terminology names might not be used in future versions as improvements are made to the Aperture Console.

About the Venafi CodeSign Protect web interface

Venafi CodeSign Protect has its own interface, which you will see only if you've licensed Venafi CodeSign Protect. The Venafi CodeSign Protect interface is where code signing projects are configured and managed, where code signing approval requests are granted, and where code signing statistics can be viewed.

If you have no other Venafi products licensed, then the code signing interface opens directly after signing into Venafi Platform. If you do have other products licensed, then you can access Venafi CodeSign Protect by clicking the Product Switcher near the top right corner.

Working with the Policy Tree

> **NOTE** Venafi is in the process of a multi-year effort to unify and modernize the server-based management consoles. As part of that effort, the terms *WebAdmin* and *Aperture* are deprecated. Just focus on the feature you need, and we'll take you to the place to do what you need to do. Some of these screens will use the "WebAdmin" look, which is now called *Policy Tree*. Other screens will look like what we used to call *Aperture*. As we continue our integration effort, eventually you'll just have one consistent UI across all of Venafi's server products.

The Venafi Trust Protection Platform™ policy tree can be accessed by connecting to the Trust Protection Platform server using a supported or compatible web browser. See System requirements for Venafi components.

This section provides an overview of the classic policy tree and reviews general management procedures.

Logging in

The first time you log in to Venafi Platform, you must use the default master administrator role (admin). The password for this account is defined during installation. For more information about the master administrator, see "Understanding system roles" on page 706.

In Trust Protection Platform, user directories are closed systems. This means that local users can see only local users and groups. Likewise, external users from a directory service can see only external users and groups within their own directory service provider.

To log in to Venafi Platform

1. Open a supported browser window and browse to the following address:

   http://*Trust Protection Platform_server*/

   > **TIP** Trust Protection Platform_server is the IP address or the hostname of the Trust Protection Platform server. Trust Protection Platform supports IPv4 or IPv6 connections.
   >
   > IPv6 addresses must be in an acceptable format: http://*Trust Protection Platform_server_IPv6_address*)/

2. In the Login dialog, do one of the following, and then click **Login**:
   - To log in to your local directory, type the administrator user name and password. If your AD connector has a Driver Loading Rank of 0, then you must log in using the Local:*username* format. For more information on connector ranking, see "Configuring the Local connection" on page 694.
   - To log in using an AD administrator account, depending on your AD environment, you can use one of the following formats:
     - SAM account name.
     - Domain name syntax (*domain_name**username*).
     - User Principle Name syntax (*valid_user*@*orgUnit.domain*.com).
     - The identity connector type plus the friendly name (*AD+friendly name*).
   - To log in using an LDAP administrator account, use the identity connector type plus the friendly name and account name (*LDAP+ODSEE:admin*).

Venafi Platform supports single sign on across products, so as you move between products, you don't have to sign in to each one individually.

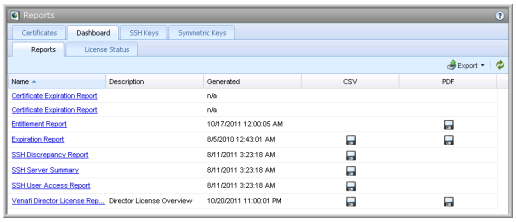
Navigating the Policy tree

The policy tree is divided into two panes: the Tree view on the left and the Detail View on the right.

On the far left, use the drop-down menu to select a different "tree" to view. Each item in this list is referred to as a "tree," so if instructions say to open the Identity tree, you'd come to the Policy Tree, then select Identity from this drop-down list.

Reports tab

The Reports tab lists all currently defined Report objects. You can click any of the report links to access the associated Report object configuration. You can also download any available report by clicking the associated download link  .



Using the Policy Tree's tree view

The tree view displays the management trees and their associated objects.

Tree	Description
Credentials	Credential objects are created and managed in the Credentials tree. Credential objects store the credentials Trust Protection Platform uses to authenticate with devices, applications, and CAs. **NOTE** Credentials can also be created and managed in the Policy tree. In the Policy tree hierarchy, Credential objects may be contained by Policy, Device, or Application objects. The ability to create Credential objects under different objects in the Policy tree facilitates the distribution of Credential object permissions assignments. For example, if you assign permissions at the policy level, then create the Credential objects under the same policy where their associated applications or certificates are located, the credentials automatically inherit the same permissions as their associated objects. In this way, you can ensure that administrators have permissions to only those credentials required to manage the applications or certificates for which they are responsible. For more information on managing your system credentials, see "Working with system credentials" on page 909.
Discovery	The Discovery tree lists the configured Discovery and Discovery Exclusion objects for network and agent-based discovery. In Policy Tree, you can do a CA Import Discovery only. All other discovery work is done in Aperture. For more information on configuring and managing discoveries in the Discovery tree, see Discovering certificates and keys.
Encryption	The Encryption tree contains your system's Encryption drivers. Encryption drivers provide access to the keys used to secure your system's encryption assets—that is, certificates, private keys, SSH keys, Credential objects, administrator usernames and passwords, and all other information stored in the Secret Store database. Trust Protection Platform uses either the Venafi Platform software key, or a hardware key on a supported HSM device (or both) to secure encryption assets within the Secret Store. For more information on managing system encryption, see "Managing system encryption keys" on page 545.
Identity	In Trust Protection Platform, all users, groups, and user datastores are managed in the Identity tree.

Tree	Description
	For more information on managing objects in the Identity tree, see "Working with identities, permissions, and teams" on page 635.
Logging	The Logging tree provides a comprehensive view of the Trust Protection Platform notification system and is the control center for all system logging and notification activities. The Logging tree lists every application that can log events in Trust Protection Platform. Each Logging Application object, in turn, stores the definitions for its associated events. This is a valuable reference when you are configuring your system notifications. The Logging tree also provides a view of all configured Notification and Channel objects. Notification objects define which types of events you want to monitor and under what conditions. Channel objects define the event output target. For more information on managing logging and system notifications, see "Understanding system logging and notifications" on page 983.
Platforms	The Platforms tree displays the Trust Protection Platform servers and modules. For example, if you have your central Trust Protection Platform server and a dedicated Discovery Server, this tree displays the two Server objects and their associated modules. From this tree, you can define global module settings like Certificate Renewal and Notification monitoring cycles, the time the Trust Protection Platform server runs its daily tasks, and the Discovery schedule.
Policy	The Policy tree provides a hierarchical view of your encryption deployment model. Policy, Jump Server, Device, Application, CA Template, Credential, Certificate, SSH Key, and Workflow objects display in context of other system objects so you can intuitively design your object hierarchy and policy inheritance paths. For information on managing folder, see "Using policies to manage encryption assets" on page 859.

Tree	Description
Reports	The Reports tree allows you to create and manage system reports. The individual Report objects–Licensing, Entitlement, Expiration and SSH Key reports–determine report format, how often the report is generated, and report delivery options. For more information, see "Managing system reports" on page 977.
Roots	The Roots tree lists all archived root and intermediate root certificates in context of their signature chain. From this tree, you can download root certificates to other servers. For more information on managing objects in the Roots tree, see Managing root certificates in the *Venafi Trust Protection Platform Certificate Management Guide*.
Workflow	Allows you to manage approval requests. The current user can manage and monitor pending Approval Requests or view a history of approved and rejected Approval Requests. For more information on implementing and managing your corporate workflow procedures, see About workflows in the *Venafi Trust Protection Platform Certificate Management Guide*.

Using the Policy Tree's view buttons

The buttons at the top of the tree view remain consistent no matter which tree is selected.

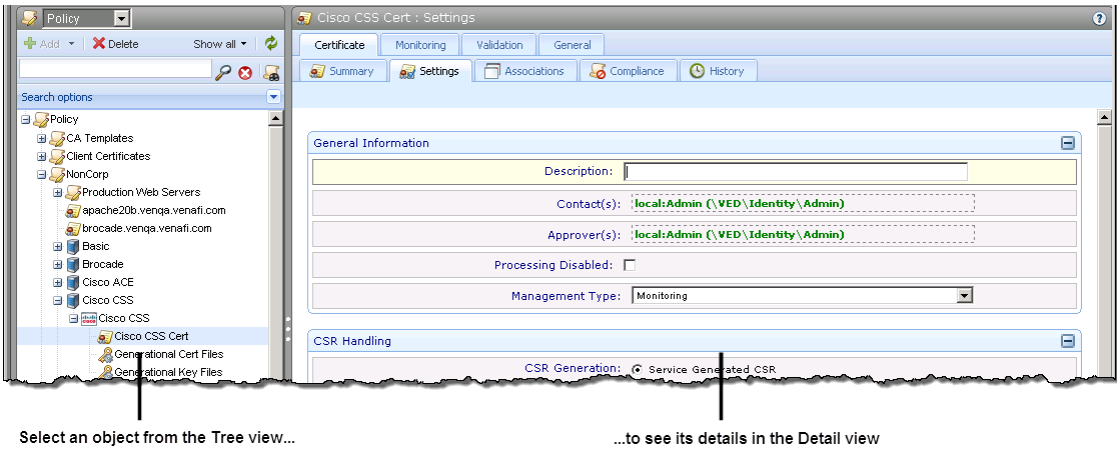
The following table describes the tree view buttons.

Button		Description
	**Add**	Adds new objects to the currently displayed management tree. The type of objects you can add depends on the selected tree.
	**Delete**	Deletes selected objects.
	Filter	Allows you to filter which objects display in the tree. For more information, see "Filtering the Tree view" on page 37.
	**Refresh**	Refreshes the contents of the current tree.

About the Policy Tree's detail view

When you select an object in the tree view, the object's corresponding configuration pages display in the Detail View. The available configuration pages, as well as the available options and settings, depend upon the object selected in the tree view. For example, if you select a certificate in the tree view, the Detail View displays the certificate's configuration options and settings.

Click the tabs along the top of the Detail View to move between configuration pages.



Policy Tree's detail view buttons

Many of the configuration pages that display in the Detail View include buttons that allow you to perform additional tasks associated with the object selected in the tree view. The buttons available on each page vary depending on the object selected in the tree view and the tab selected in the Detail View.

The Summary tab for a certificate is displayed in the Detail View. The tab includes the following buttons:

- Restart
- Retry
- Print
- Refresh

The following table reviews all the buttons that appear on the various configuration pages in the Detail View when you select objects in the tree view. Not all of these buttons appear on every page.

Button		Description
	**Add**	Adds new entries to the current page in the Detail View. This button is available on the following tabs: ■ Permissions–Available with any object you select in the tree view. Allows you to assign user and group permissions to the selected object. ■ Associations–Available with a selected Certificate object in the Policy tree. Allows you to associate new applications with the selected Certificate object.
	Approve	Approves the selected pending request. This button is available only on the Pending Request tab, which is accessible from the Approvals tree.
	**Delete**	Deletes the selected objects from the current Detail View page. This button is available on the following tabs: ■ Permissions–Available with any object you select in the tree view. Allows you to unassign user and group permissions from the selected object. ■ Associations–Available with a selected Certificate object in the Policy tree. Allows you to delete applications associated with the selected Certificate object.
	Download	Allows you to download certificates. This button is available only on the Certificate tab, which can be accessed when a Certificate object is selected in the Policy tree.
	**Enable**	Toggles between enabling and disabling the processing of certificates in the selected Application objects.
	**Disable**	This button is available on the Associations tab, which can be accessed when a Certificate object is selected in the Policy tree.
	**Export**	Exports the data displayed in the current Detail View to a CSV, tab-delimited, HTML, or XML file. This button is available on the following tabs: ■ Permissions–Available with all objects in every management tree. Exports

Button	Description
	users and groups and the permissions assigned to each user and group. ■ Log–Available with objects in the Policy, Discovery, and Reports tree. Exports a list of all events triggered by the current object. ■ All Certificates–Available when you select a Policy object in the Policy tree. Exports a list of the policy's subordinate certificates. For more information, see Opening the certificate inventory in the *Venafi Trust Protection Platform Certificate Management Guide*. ■ Associations–Available when you select a Certificate object in the Policy tree. Exports a list of all the applications the current certificate is installed on. For more information, see Associating certificates with applications in the *Venafi Trust Protection Platform Certificate Management Guide*. ■ History–Available when you select a Certificate object in the Policy tree. Exports the common name, serial number, issuer, and valid dates for each edition of the certificate associated with the current Certificate object. For more information, see About Viewing Certificate History in the *Venafi Trust Protection Platform Certificate Management Guide*. ■ All Roots–Available when you select a Root object in the Roots tree. Exports a list of all archived root and intermediate root certificates in context of their signature chain. For more information, see Managing root certificates in the *Venafi Trust Protection Platform Certificate Management Guide*. ■ Requests–Available in the Workflow tree. Exports a list of the current user's approved, pending, or rejected requests. For more information, see About workflows in the *Venafi Trust Protection Platform Certificate Management Guide*. ■ Plugins–Available when you select the Root Configuration object in the Configuration tree. Exports a list of all Trust Protection Platform plug-ins. ■ Users & Groups–Available when you select the Local or an Active Directory

Button	Description
	Connection object in the Identity tree. Exports a list of all users and groups in the current user directory. For more information, see "Working with identities, permissions, and teams" on page 635. ■ Group Members–Available when you select a Group object in a user directory. Exports a list of all members of the current group. For more information, see "Working with identities, permissions, and teams" on page 635. ■ User Entitlements–Available when you select a User object in a user directory. Exports a list of the objects the current user has been granted explicit permissions to. For more information, see About viewing user entitlements. ■ Identity Mapping Table–Available when you select the Local or an Active Directory Connection object in the Identity tree. Exports the attribute mapping rules defined for the current user directory. For more information, see "Defining mapping rules for Local user and group attributes–Mapping Table tab" on page 696. ■ Discovery Results–Available when you select a Discovery object in the Discovery tree. Exports a list of all certificates discovered on the IPv4 addresses and ports defined in the current Discovery object. For more information, see or .
 **Extract**	Extracts the certificate and private key installed on the selected Application objects. Trust Protection Platform compares the extracted certificate and private key with the current certificate. If there is a mismatch, Trust Protection Platform asks if you want to overwrite the current certificate and private key. This button is available only on the selected Certificate object's Associations tab.
 **Include Sub-folders**	Displays the certificates of the current policy only or all certificates below the current policy, including those in subfolders. This button is available only on the selected Policy object's All Certificates tab.

Button		Description
	**Import**	Allows you to import existing certificates from the local machine or a server on the network. This button is available only on the selected Certificate object's Certificate tab.
	**Move Down**	Moves the selected plug-in down in priority. This button is available only on the Plugins tab, which can be accessed from the Configuration tree.
	**Move Up**	Moves the selected plug-in up in priority. This button is available only on the Plugins tab, which can be accessed from the Configuration tree.
	**Print**	Prints the contents of the current Detail View. This button is available on many pages in the Detail View.
	Push	Pushes the current certificate and private key to the selected application. **IMPORTANT** If the certificate and private key already exist on the target server, the push operation replaces the existing certificate and private key. Trust Protection Platform does not process a push operation unless the following conditions are met: ■ The certificate is available in the Trust Protection Platform database ■ The certificate's management type is Provisioning ■ The certificate is not currently being processed ■ This button is available only on the selected Certificate object's Associations tab.
	**Refresh**	Refreshes the contents of the current page or tree. When you click Refresh, any data cached on the server for the current page or tree is also cleared or reset. Additionally, the user's permissions are reloaded and refreshed on all trees and on the Permissions tab. This button is available on most pages in the Detail View.

Button		Description
	**Reject**	Rejects the selected pending request. This button is available only on the Pending Requests tab, which is accessible in the Approval tree.
	**Renew Now**	Queues the certificate for renewal. This button is available only on the selected Certificate object's Settings tab.
	**Reset**	Clears errors and stages on the certificate and its associated applications, then stops processing. This button is available only on the selected Certificate object's Summary tab.
	**Restart**	Clears all errors and stages on the certificate and its associated application(s), then restarts processing from the beginning. Each stage is retried. This button is available only on the selected Certificate object's Summary tab.
	**Retry**	Clears the certificate error, then retries the last processing stage. This button is available only on the selected Certificate object's Summary tab.
	**Retry Installation**	Reattempts to install the certificate on the associated application's server. This button is available only on the selected Certificate object's Associations tab.
	**Revoke**	Submits a revocation request to the certificate CA. This button is available only on the selected Certificate object's Summary and History tabs.
	**Show Intermediate Root Certificates**	Displays either root certificates only or all intermediate root certificates as well. This button is available only on the selected Root object's All Roots tab.

Adding objects to the policy tree

You can easily add new objects to management trees in the policy tree. The type of objects you can add depends on which tree is displayed and the object selected in the tree. For example, if the Credential tree is displayed, you can add Password, Username, Certificate, or Private Key credential objects. If the Policy tree is displayed, you can add Certificate, Device, or folder.

Some objects, such as Credential objects, can be added only at the root of their respective trees. Others, such as Certificate and Application objects, can be added to objects.

You can add objects by clicking the **Add** button at the top of the tree view, the **Add** drop-down menu, or the right-click menu.

> **NOTE** The right-click menu is not available in all trees.

If a new object cannot be added to the selected object, the **Add** drop-down menu and the right-click menu are not accessible.

To add an object using the Add button

1. From the TLS Protect menu bar, click **Policy Tree**.

   You must have the Create permission to the folder where you want to add an object.

2. From the **Tree** drop-down menu, select a tree.
3. In the **Tree** view, select the object where you want to create the new object, and then click **Add**.

   The types of objects that can be added under the selected object display.

   +

4. In the **Create a new object** pane, click the type of object you want to add.
5. Define the new object's parameters and settings.
6. Click **Save**.

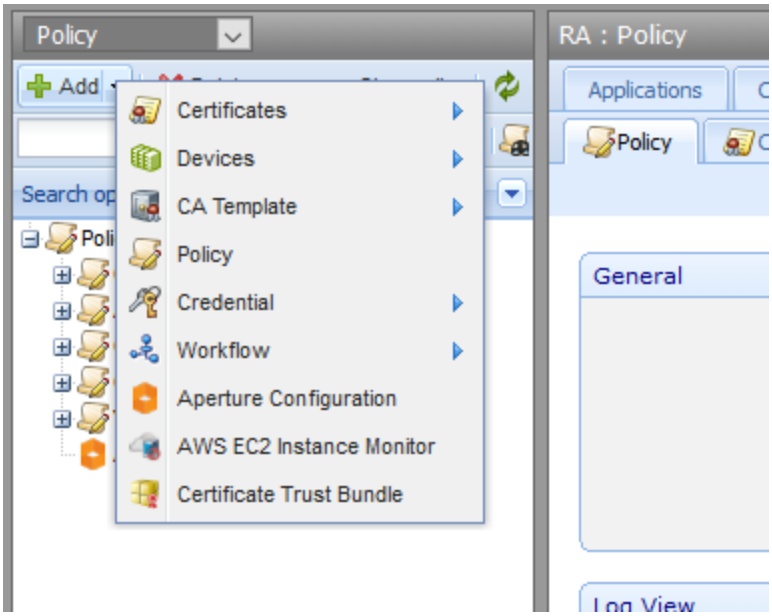
The new object is added to the tree view.

To add an object using the Add drop-down menu

1. From the TLS Protect menu bar, click **Policy Tree**.

   You must have the Create permission to the folder where you want to add an object.

2. From the **Tree** drop-down menu, select a tree.
3. In the **Tree** view, select an object.
4. Click **Add**, and then select the type of object you want to create.



5. In the **Detail** View, define the new object's parameters and settings.
6. Click **Save**.

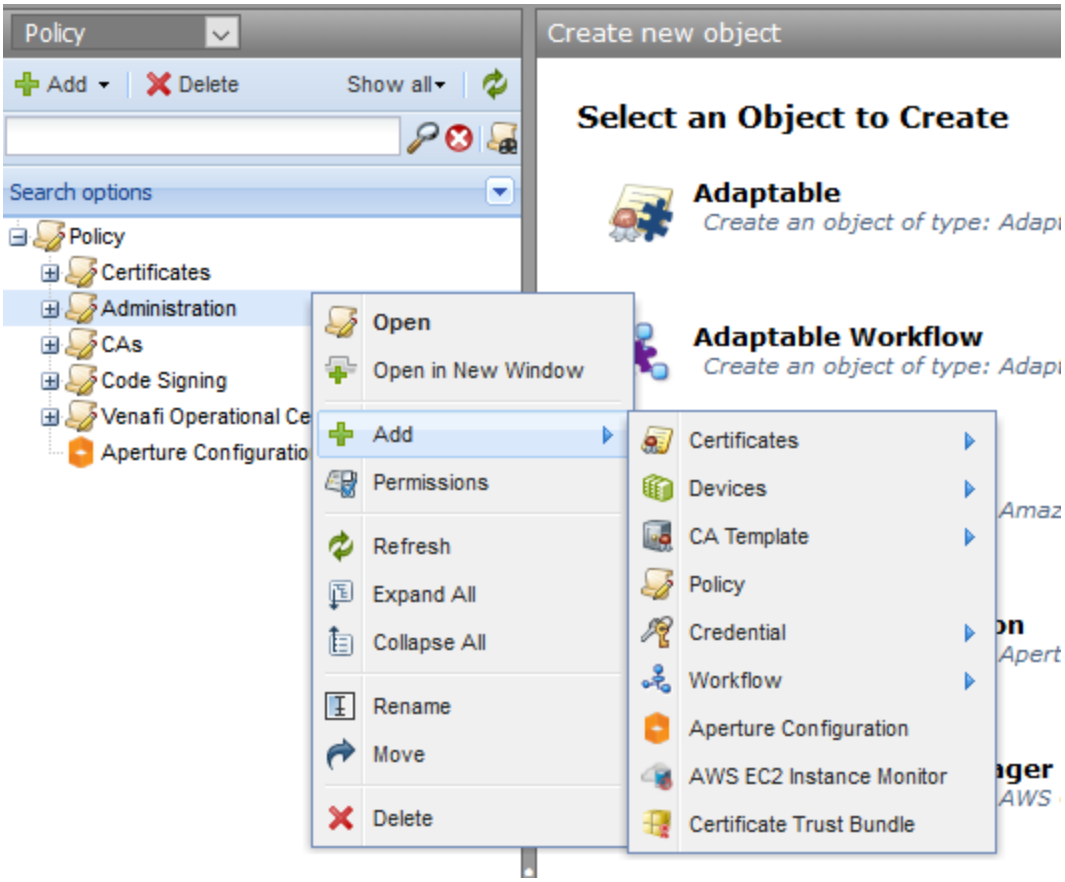
The new object is added to the tree view.

To add an object using the right-click menu

1. From the TLS Protect menu bar, click **Policy Tree**.

   You must have the *Create* permission to the folder to which you want to add the object.

2. From the **Tree** drop-down menu, select a tree.
3. In the **Tree** view, right-click the folder where you want to create the new object, and then click **Add** > *object*.



4. In the **Detail** View, define the new object's parameters and settings.
5. Click **Save**.

The new object is added to the **Tree** view.

Deleting objects

You can delete objects that you no longer need to manage; however, not all objects can be deleted. For example, you cannot delete default root objects in any tree and you cannot delete the default Admin or local objects from the Identity tree.

You can use the Delete button or the right-click menu.

To delete an object using the Delete button

1. From the TLS Protect menu bar, click **Classic Policy Tree**.

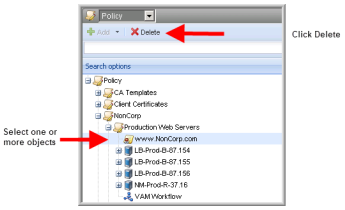
   You must have Delete permissions to the object(s) you want to delete.

2. From the **Tree** drop-down menu, select a tree.

3. In the **Tree** view, select the object(s) you want to delete.

   Press **Shift+click** to select multiple, contiguous objects.Press **Ctrl+click** to select multiple, discontiguous objects.

4. Click **Delete**.



5. Click **Yes** to confirm.

   The object is removed from the tree view.

WARNING! If you delete a folder object, all child objects are also deleted. A warning dialog appears asking if you are sure you want to delete the object and all child objects. Click **Yes** to delete the objects. Click **No** to return to the management tree.

To delete an object using the right-click menu

1. From the TLS Protect menu bar, click **Classic Policy Tree**.

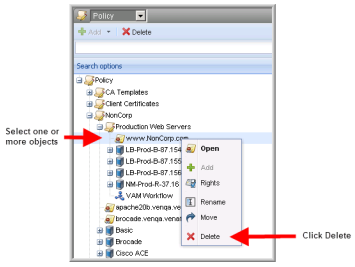
   You must have Delete permissions to the object(s) you want to delete.

2. From the **Tree** drop-down menu, select a tree.

3. In the **Tree** view, select the object(s) you want to delete.

   Press **Shift+click** to select multiple, contiguous certificates.

   Press **Ctrl+click** to select multiple, discontiguous certificates.



4. Click **Yes** to confirm.

The object is removed from the tree view.

If you delete a folder object, all child objects are also deleted. A warning dialog appears asking if you are sure you want to delete the object and all child objects. Click **Yes** to delete the objects. Click **No** to return to the management tree.

Moving objects

Objects in the Policy tree can be moved from one folder to another if the target folder supports the type of object being moved.

You must have *Rename* permissions to the objects you want to move and *Create* permissions to the target folder.

> **TIP** When you move a folder, all sub-folders and objects contained in it are moved also.

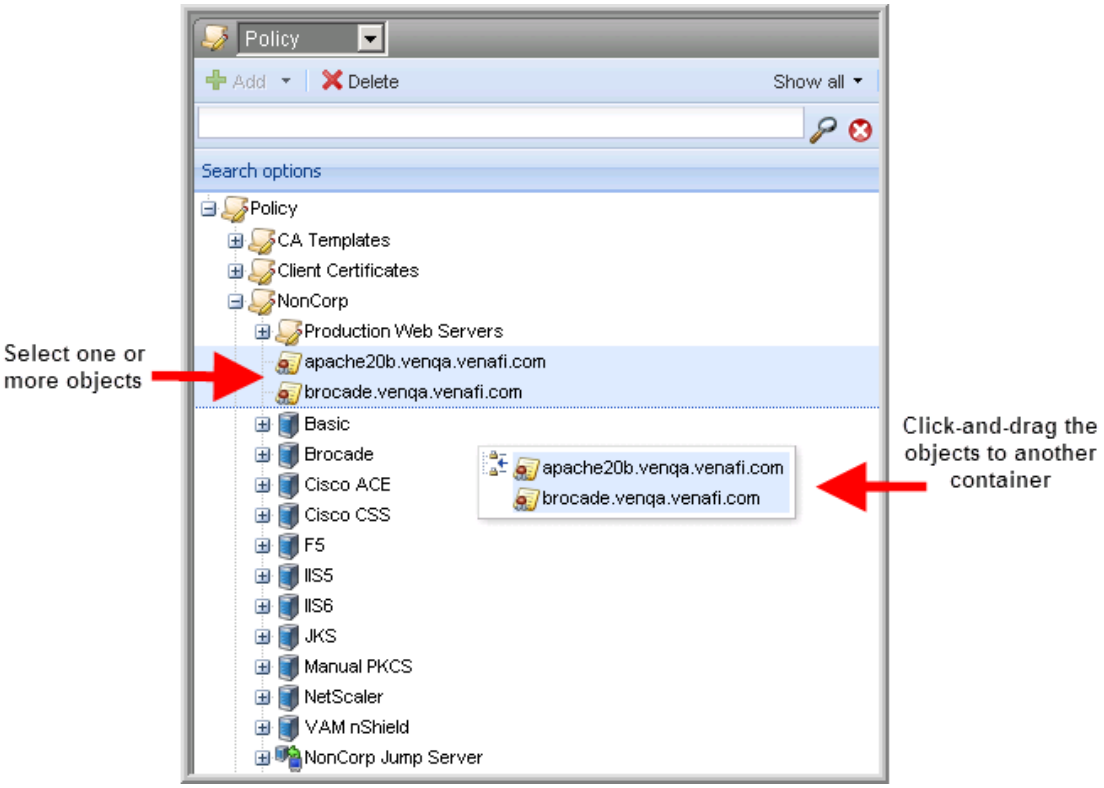
To move an object using click-and-drag

1. From the TLS Protect menu bar, click **Classic Policy Tree**.
2. From the **Tree** drop-down menu, select a tree.
3. In the **Tree** view, select the object(s) you want to move.

   Press **Shift+click** to select multiple, contiguous certificates.

   Press **Ctrl+click** to select multiple, discontiguous certificates.
4. Click and drag the selected object to another folder in the tree.

   When an object is moved, locked policy attributes are recalculated.

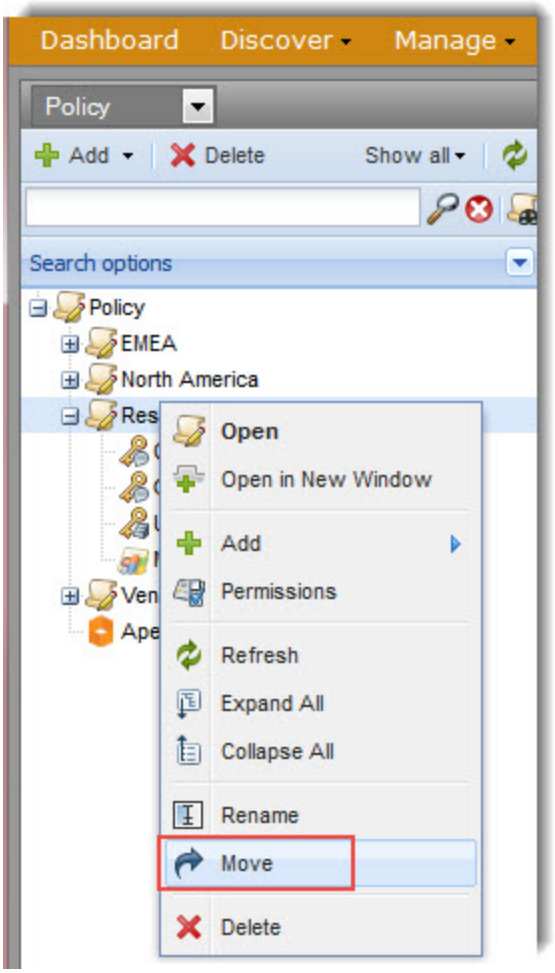


To move an object using the right-click menu

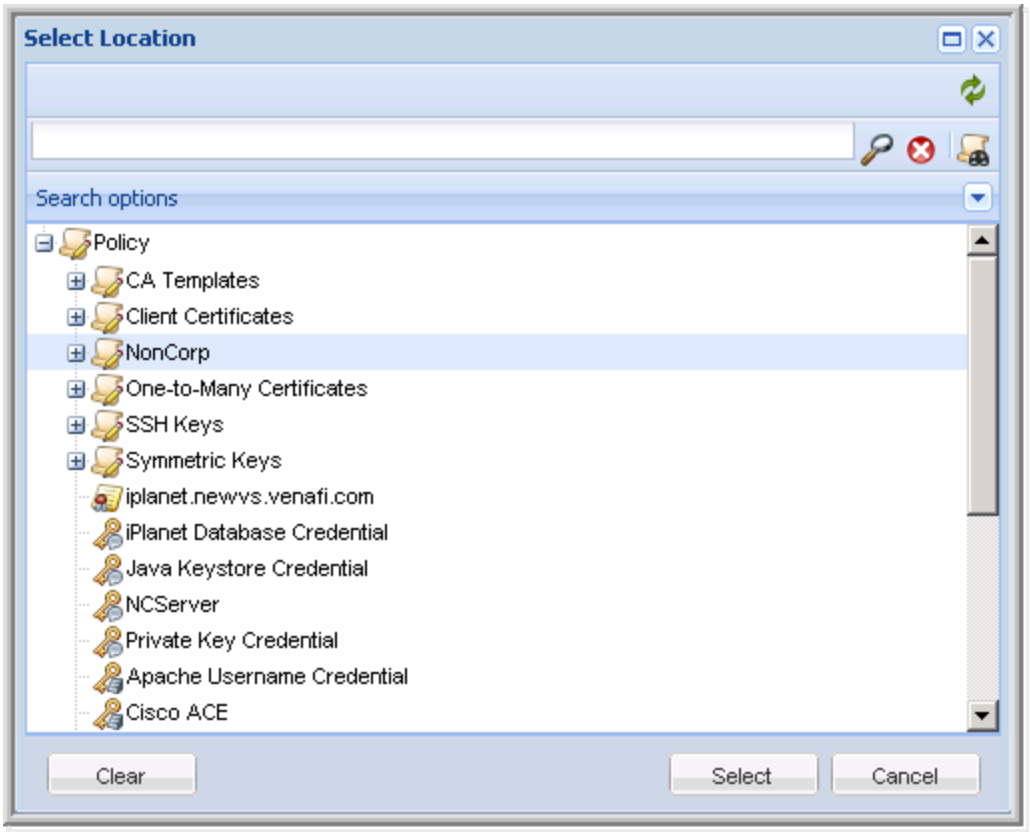
1. From the TLS Protect menu bar, click **Classic Policy Tree**.
2. From the **Tree** drop-down menu, select a tree.
3. In the **Tree** view, select the objects you want to move.

   Press **Shift+click** to select multiple, contiguous certificates.

   Press **Ctrl+click** to select multiple, discontiguous certificates.
4. Right-click the selected objects, and then click **Move**.



5. In the **Select Location** dialog box, click **Select** to move the objects to the selected folder.



Renaming objects

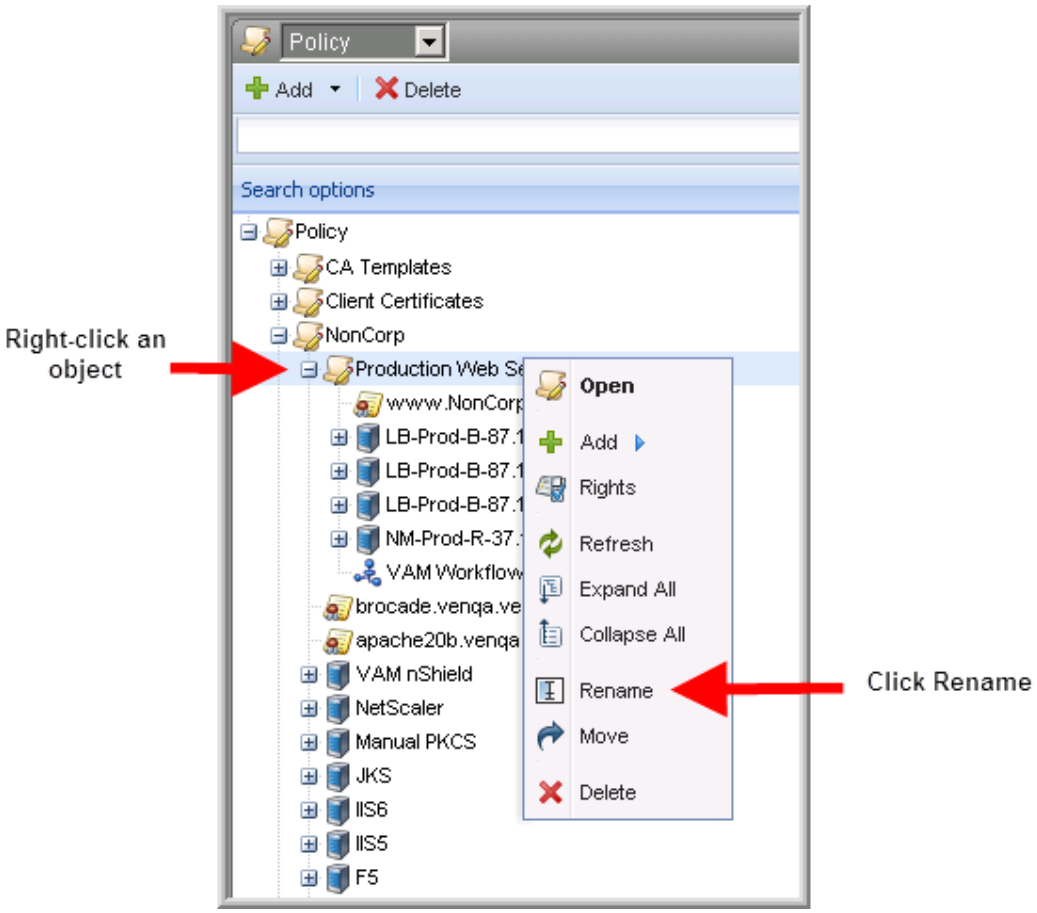
You can rename items in the management trees at any time. A quick method for renaming items is to use the right-click menu.

You must have *Rename* permissions to the object you want to rename.

> **NOTE** Not all objects can be renamed. For example, you cannot rename root objects, or the first folder in a management tree. You also cannot rename any items on the Approvals tree.

To rename an object

1. From the TLS Protect menu bar, click **Classic Policy Tree**.
2. From the **Tree** menu, select a tree.
3. In the **Tree** view, right-click the object you want to rename, and then click **Rename**.



4. In the **Rename Object** dialog, type the new name, and then click **OK**.

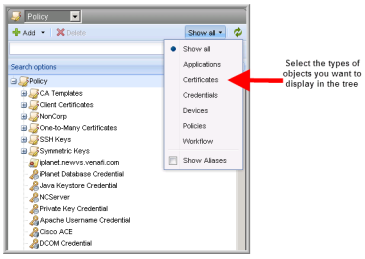
IMPORTANT If you rename an object in the Policy tree, and you have placement rules that place objects in that object, the next time the placement rule is run, the old object will be recreated and the devices and certificates that are placed will be placed in the old object. Therefore, when you rename an object, you should check the placement rules settings to make sure you don't have any placement rules that direct objects to the folder you are renaming. If you do, make sure to update the placement rules to the new object name. For more information see Network placement rules in the Certificate Management Guide.

Filtering the Tree view

You can use the **Filter** button to display only specific kinds of items in the Tree view. The button toggles between a Show All and Filtered state. When no filter is applied, the button reads Show All. When the objects are filtered, the button reads Filtered.

To filter objects in the tree view

1. From the Platform menu bar, click **Policy Tree**.
2. From the **Tree** menu, select a tree.
3. Click the **Filter** button, and then select the types of items you want to display in the tree.



The tree view refreshes and displays only the type of objects you selected and to which you have View permissions.

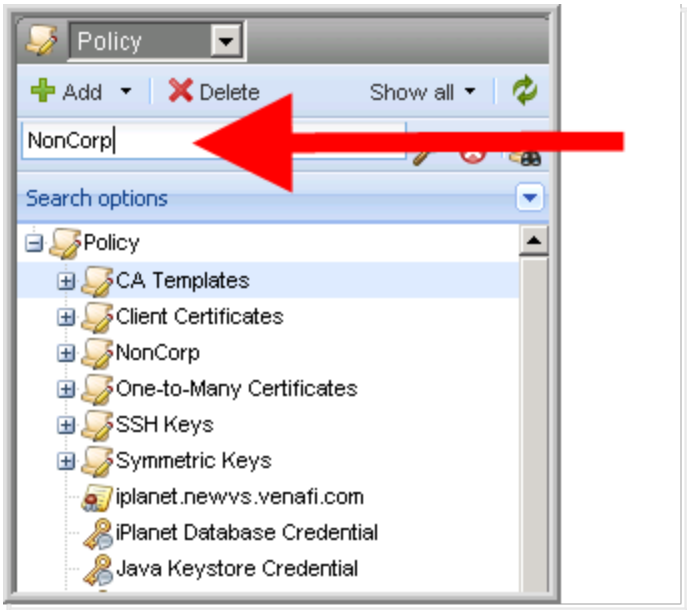
Searching the policy tree

To accommodate customers with large numbers of items in their Policy tree, Trust Protection Platform now has advanced search capabilities. Administrators can search for specific objects within the tree as well as attributes within objects using “Starts with” or “Contains” operators.

To search the policy tree

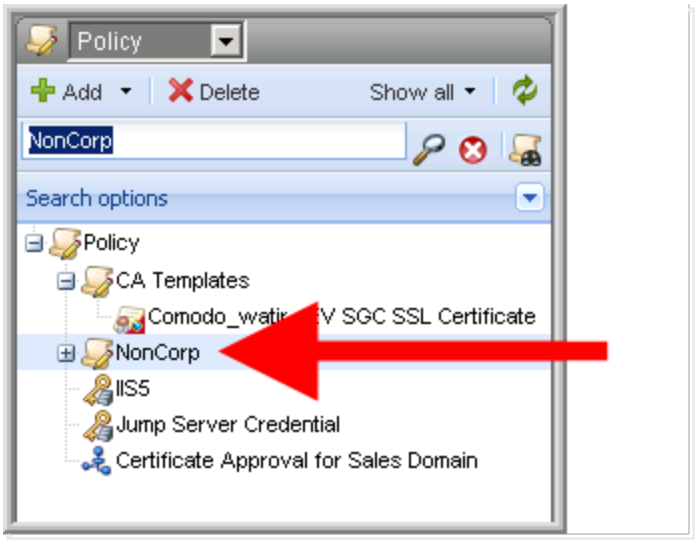
1. From the Platform menu bar, click **Policy Tree**.
2. Enter a search string in the search field, then press <Enter> to initiate the search.

   You can use wildcard characters in the search string.



3. The list shows any object to which you have View permissions and whose name matches the designated search parameter.

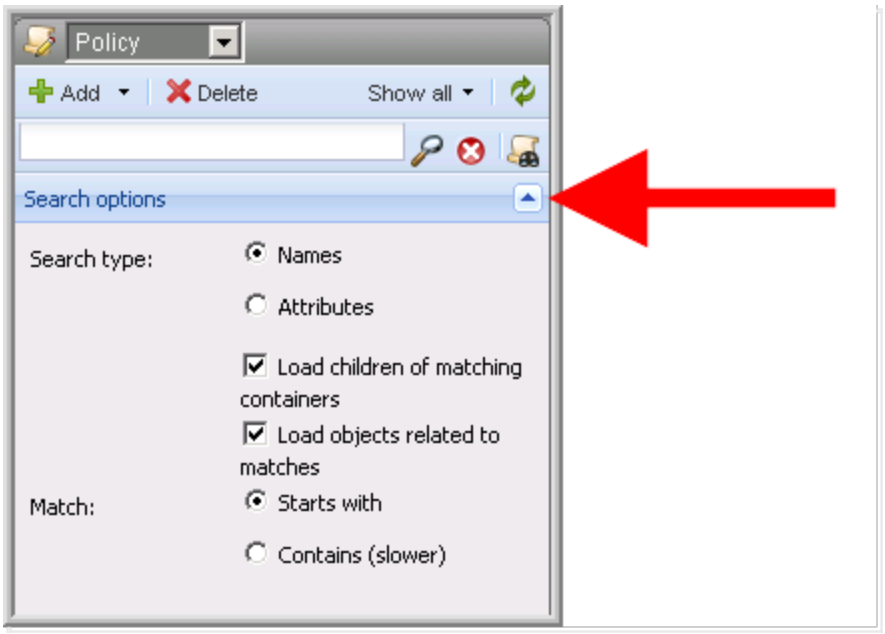
   By default, the search also returns any child objects as well as objects related to the search results.



To define search options

1. From the Platform menu bar, click **Policy Tree**.
2. Select a tree.

3. Click the **Search Options** menu to expand the search options.



The search options menu appears.

4. Designate your search parameters:

Search Option	Description
Search Types	
Names	Searches for object names that match the designated parameters. This option is enabled by default.
Attributes	Searches for object attributes that match the designated parameters.
Load children of matching folders	Returns the child objects for any object(s) matching the designated search parameters. For example, if the search returns an Application object, the administration console would also display the Application's child Certificate object. This option is enabled by default.

Search Option	Description
Load objects related to matches	Returns objects related to any object(s) matching the designated search parameters. For example, if the search returns an Application object, the administration console would also display the parent Device and folder as well as the child Certificate object, its associated CA template object and any other Application objects associated with the Certificate object. This option is enabled by default.
Match	
Starts with	Finds only objects whose name or attribute begins with the designated parameters.
Contains	Finds objects whose name or attributes contain the designated parameters.

5. Enter the search criteria, then press <Enter> or click  to initiate the search.
6. You can use wildcard characters in the search string.
7. The search shows any object that matches the designated criteria and to which the current user has View permissions.
8. To clear a search query, click  .

Start the console in Query mode

To minimize the amount of data the administration console has to pull from the database each time it loads or refreshes the Policy tree, you can configure the administration console to launch in query mode rather than browse mode. You can then enter a query for a specific object, object class, or object attribute. The query results include only the objects for which the administrator has View permissions. This option is designed especially for organizations with large Policy trees.

To configure the classic policy tree to launch in Query mode specific to user

1. From the TLS Protect menu bar, click **Classic Policy Tree**.
2. From the **Policy** tree menu, click **Show All**.
3. Check the box next to **Support Large Object Trees**.

From now on, for the specific user, the classic policy tree will open the Policy tree in browse mode. No objects display in the tree until after you enter a search query.

To configure system-wide account settings to launch in Query mode

Administrators can force all users' administration consoles to launch in Query mode by enabling the **Support large object trees** option in the root folder of the **Platforms** tree (**Platforms** tab, **Settings** sub-tab, **Global Options** group).

The global **Support Large Object Trees** setting is also available thru the admin console by clicking the account icon > **Preferences** > **TLS Protect & Client Protect**. See "Preferences" on page 11.

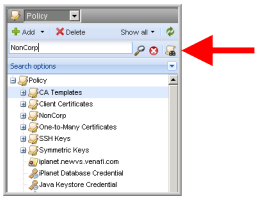
Finding objects in the Policy tree

In addition to its search capabilities, Trust Protection Platform provides a **Find** function to locate specific objects in the Policy tree.

To find an object in the Policy tree

1. From the Platform menu bar, click **Policy Tree**.
2. Enter a search string in the search field.

   Wildcard characters may be used in the search string.
3. Click the Find icon.

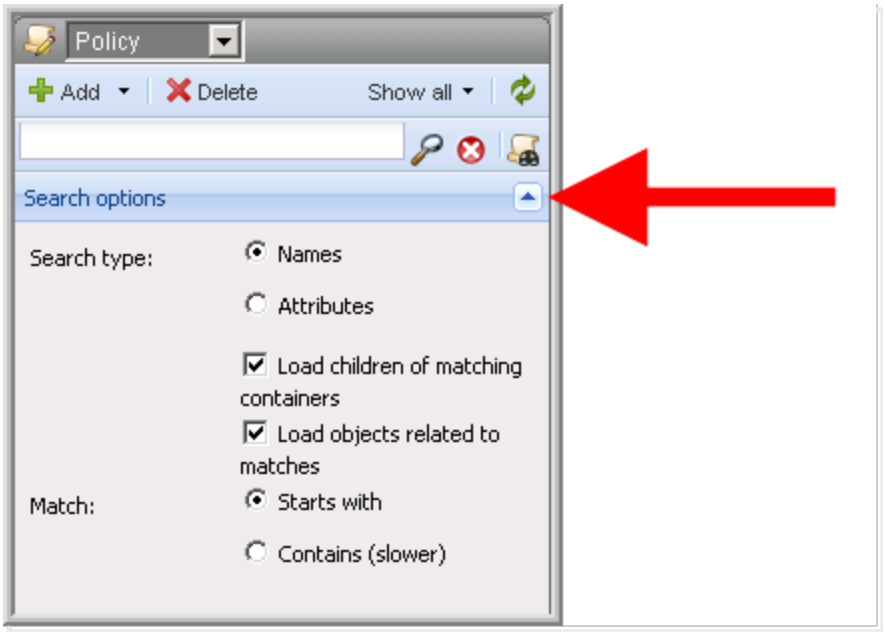


   When you initiate a Find, Trust Protection Platform starts at the top of the tree, then finds the first object that begins with the designated search string and to which the current user has View permissions.
4. (Optional) Press <Enter> to find the next object in the Policy tree as per the designated parameters.
5. Continue pressing <Enter> to cycle through the tree and find all objects that meet the designated parameters.

By default, the Find function defaults to performing a “begins-with” search; however, you can also use the Search Options menu to specify a “contains” search.

To find an object in the Policy tree using a *contains* search

1. In the **Tree** menu, select a tree.
2. Click the **Search Options** menu to expand the search options.



3. Select the **Contains** option to find objects whose name contains the designated search string.
4. Enter a search string in the search field.

   Wildcard characters may be used in the search string.
5. Click the Find icon.

   Trust Protection Platform starts at the top of the tree, then finds the first object that begins with the designated search string and to which the current user has View permissions.
6. (Optional) Press <Enter> to find the next object in the Policy tree that contains the designated search string.
7. Continue pressing <Enter> to cycle through the tree and find all objects that contain the designated search string.

Venafi Configuration Console

The Venafi Configuration Console (VCC) provides an overview of your system, and allows you to control and configure many aspects of your Venafi Trust Protection Platform installation.

Using this console, you can manage configuration items from the following categories:

- **Attention Required**: View a consolidated summary of issues that require your attention.
- **Database**: View and edit the database connection information.
- **Product**: Enable, disable, remove, and add Venafi Platform components and edit licenses.
- **Connectors**: View, add, edit, and remove connectors, including encryption connectors, identity connectors, and credential connectors (e.g. CyberArk).
- **System Roles**: View and assign system roles to users and groups.
- **Authentication**: Create and manage third-party authentication methods (e.g. SAML).
- **Recycle Bin**: A utility that allows administrators to undo the deletion of the system's most critical objects. It includes the ability to automatically remove expired certificate data from secret store.
- **Access Management**: Configure and manage access to Venafi Platform by way of Venafi's public APIs.
- **Code Signing**: Create, edit, and delete templates and configuration options to be made available when code signing projects are requested. This node requires a Venafi CodeSign Protect license. See the CodeSign Protect administration steps for details.
- **Events**: View logs of Trust Protection Platform events and create custom views of events. See "Venafi Event Viewer" on page 374 for details.
- **Statistics**: View detailed statistics of Trust Protection Platform activity and performance. See "Venafi Statistics Viewer" on page 384 for details.
- **Message Bus**: A utility that provides near-instant notification to other servers in the cluster about significant changes to the database by way of an MQTT message broker.
- **Tools**: Access to tools, such as Logging, which allow you to manage your environment. The Logging tool controls all notifications and logging features of Venafi Platform including e-mail templates and e-mail notifications.

The configuration console is based on the Microsoft Management Console, providing a familiar interface for Windows administrators to accomplish system maintenance tasks.

The left panel shows the nodes you can interact with. The center panel shows information about the selected node. The right panel shows actions you can take on a selected item.

This chapter contains the following topics:

Answer File wizard

An answer file is an XML-based file that contains configuration information for your installation of Venafi Platform. It includes the enabled modules, database connection information, and security keys used for the configuration. Using an answer file during installation makes it easy to use the same installation settings across multiple servers in your Venafi Platform cluster. An answer file is also helpful for upgrading your system, if you use a non-traditional upgrade method. For more information about answer files, see Creating and using answer files.

The answer file can be generated in two different ways. If you have installed Venafi Platform, you're probably aware of the ability to create an answer file when you install Trust Protection Platform using the GUI.

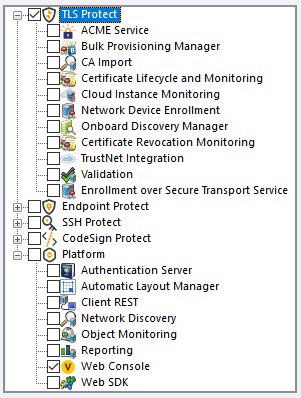
You can also generate an answer file from the Venafi Configuration Console once you have installed Venafi Platform on a server. This topic discusses how to create an answer file using the Answer File Wizard in the configuration console.

To generate an answer file using Venafi Configuration Console

1. Log in to the Venafi Platform Windows server and launch **Venafi Configuration Console**.
2. [Optional] If you want to **Disable validation of the provided** values, check the box.

   Generally, you will want to validate the values as you enter them into the answer file wizard. However, if you are configuring for a server in a different zone (say a production server that you can't access due to the network configuration), you will want to disable validation so the system doesn't provide an error when you enter connection information that can't be verified.
3. From the root **Venafi Configuration** node in Venafi Configuration Console, click **Run Answer File Wizard** in the Actions panel on the right.
4. Click **Next**.
5. [Optional] If you already have an answer file as a template, on the **Answer File** tab click the **Browse** button to locate the answer file. If the answer file is encrypted with a password, enter the password, then click **Next**.
6. On the **Component Selection** tab, use the tree to select which components and features you want to enable for the installation.

IMPORTANT The installation will not work properly unless you select at least one product (TLS Protect, Client Protect, CodeSign Protect, or SSH Protect). If you are trying to install a UI-only server (WebConsole) you need to select one top-level product, in addition to the UI components in the Common Components list. However, in that case, you can deselect the child components of the top-level product. For example, this is a valid configuration:



Select the components you want to install, then click **Next**.

7. On the **Hardware Encryption** tab, determine if you want to use hardware encryption.

   Venafi Trust Protection Platform can encrypt data using one or more keys stored in an HSM. For code signing, Venafi Trust Protection Platform can use private keys stored on an HSM to sign code. To enable hardware encryption, check the box, and fill out the requested information.

Hardware encryption field descriptions

Field	Description
Name	Name of the HSM connector. This name will be how Master Admins identify this HSM connector when they are creating environment templates. In this example, we'll name it Default HSM.
Cryptoki DLL Path	Trust Protection Platform requires access to the 64-bit version of Cryptoki DLL. For SafeNet Luna SA devices, this is the path to the `cryptoki.dll` file. For Entrust nShield Connect HSM devices, this is the path to the `cknfast.dll` file. After selecting the DLL, click **Load Slots**. Trust Protection Platform will query the HSM and return the available slots.

Field	Description
	IMPORTANT Trust Protection Platform requires the path to the DLL file to initialize the connection to the HSM device. This path will be used for all Trust Protection Platform servers in the cluster (connected to the same database). All servers in the cluster must have their DLL file in the same location.
Slot	Slot ID for the HSM partition where you want Trust Protection Platform to access the encryption keys. **NOTE** While slot numbers are listed in the drop-down list, Trust Protection Platform does not depend on slot numbers. Trust Protection Platform identifies HSM partitions by label first, and in the case that there are duplicate labels, it falls back to the serial number.
User Type	User type required to access the HSM keys on the designated partition (Slot ID). The designated User Type must have sufficient permissions to use the keys in the Encryption Driver's Permitted Keys list.
Pin	Pin, if one is required to access the HSM. If you use Entrust nShield token protection, leave the field empty. If you are setting up AWS CloudHSM, the pin must be in the following format: `<CU_user_name>:<password>`.
Default key	The default encryption key used by the system. If you are adding a server to an existing database, you cannot change this selection. This is also the key used to protect the database connection string stored in the registry.
Create (button)	If you want to generate a new AES 256-bit symmetric key on the HSM, click this button. A new key will be generated.

NOTE In the table above, if you chose to disable validation, the **Default Key** field is a text field, and there is no **Create** button.

TIP If you are installing to an existing database, if hardware encryption is enabled, you will need to enter the PIN to continue, even though no other information appears on the screen.

NOTE You must select either one or both encryption types (hardware and/or software encryption).

IMPORTANT The keys used to encrypt Trust Protection Platform are critical to the system's functionality. Without the encryption keys, you cannot access the database or stored secrets.

8. On the **Software Encryption** tab, determine if you want to use software encryption.

   Venafi Platform can encrypt data using a software encryption key.

   If you are connecting to a new database, you can either provide a key, or have one generated for you.

   If you are connecting to an existing database, you must use the software key used to encrypt that database.

Software encryption field descriptions

Field	Description
Generate a New Key	Choose this option if this is a new installation and you want the system to generate a new, unique key for this database. Use this if you want to create a totally separate Venafi Platform system. A random password will be generated and stored in the answer file.
Use Local System Key	Chose this option if you want to use the key from the currently-running server. This saves you the effort of locating, extracting, and reusing the existing key.
Use Shared Key	Choose this option if you are connecting to an existing database secured by a software encryption key, or if you have an existing key you want to use.
Key Password	(Only if using Shared Key option) If the key is encrypted with a password, enter the key's password.
Encoded Key	(Only if using Shared Key option) Enter or paste the entire encryption key (including the ---- Begin --- and ---End--- lines).

If you are connecting to an existing database (and you chose to validate the answer file) with software encryption enabled, before you can move to the next tab, the system will verify that the software key matches the existing database's software encryption key.

TIP If you are installing with an existing database, if software encryption has not been configured for that database, the options on this screen will be disabled.

NOTE You must select either one or both encryption types (hardware and/or software encryption).

IMPORTANT The keys used to encrypt Trust Protection Platform are critical to the system's functionality. Without the encryption keys you cannot access the database or stored secrets. Consequently, if you use a software encryption key, it is highly recommended that you back up

the key to a secure location. In the event of a system failure, you can restore the key so Trust Protection Platform can access your system data.

9. On the **Database Settings** tab, choose either the Settings tab or the Expert tab, and fill out the connection information for your database. If you enter different data into both tabs, the tab you are on when you click **Next** will determine which settings are applied.

   Before you configure a new database connection, you must have previously created the Trust Protection Platform database and configured both database service accounts.

   For information about the types of database service accounts and permissions they need, see Setting up your Microsoft SQL database server.

Field descriptions - Settings tab

Field	Description
Hostname	Enter the hostname, FQDN, or IP address for the database connection. **NOTE** If you enable the TLS encrypted connection, you will need to enter the FQDN that matches the certificate presented by the MSSQL server.
Port	Enter the database port number. The default port is 1433.
Database	Enter the name for the VenafiTrust Protection Platform database.
Server supports TLS encrypted connections	Enabling this option encrypts all communications between the Venafi Platform server and the back end database. If this option is not selected, the credentials are still protected but all other communications between the server and the database might not be protected. Recommendation: Enable
Enable AlwaysOn Availability Groups	The Always On Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. When using this setting, use the virtual server name of the availability group listener in the hostname field.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>CAUTION Using AWS Multi-AZ (Availability Zone) requires special configuration including creating a virtual private cloud (VPC) with both private and public subnets. Please contact Venafi Customer Support for additional configuration instructions.</td></tr>
<tr><td>Database Owner Account fields</td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Type</td><td>Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list.

Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.</td></tr>
<tr><td>Login</td><td>Enter the account name that has the required permissions.

If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account.

If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede$</code>. Don't forget the trailing <code>$</code>.</td></tr>
<tr><td>Password</td><td>Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Operational Account fields</td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Type</td><td>Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list.

Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.</td></tr>
<tr><td>Login</td><td>Enter the account name that has the required permissions.

If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account.

If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede$</code>. Don't forget the trailing <code>$</code>.</td></tr>
<tr><td>Password</td><td>Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.</td></tr>
</table>

NOTE The lowest level of database grants that the operational account requires is automatically provided by Trust Protection Platform through the database owner account.
</td></tr>
</table>

Field descriptions - Expert tab

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Database Owner Account</td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Connection String</td><td>The connection string is a combination of the database settings selected above.

This option is most commonly used if your database administrator instructs you to use a connection string with additional parameters that aren't available in the Venafi Configuration Console user interface.</td></tr>
<tr><td>Password</td><td>The password to connect to the database.

If there is a password provided in the connection string, that password will be used for the connection, regardless of what is set in the Password field.</td></tr>
</table>
</td></tr>
<tr><td>Operational Account</td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Connection String</td><td>The connection string is a combination of the database settings selected above.

This option is most commonly used if your database administrator instructs you to use a connection string with additional parameters that aren't available in the Venafi Configuration Console user interface.</td></tr>
<tr><td>Password</td><td>The password to connect to the database.

If there is a password provided in the connection string, that password will be used for the connection, regardless of what is set in the Password field.</td></tr>
</table>
</td></tr>
</table>

If you are connecting to an existing database and you chose to validate the answer file, before you can move to the next tab, the system will verify that the database connection information is correct.

10. On the **Administrative Account** tab, enter information for the local master admin account for Venafi Trust Protection Platform.

    You need to create a local master admin account for Trust Protection Platform. You will use this account to log in to Trust Protection Platform and to perform maintenance and upgrade tasks in the system. The local master admin account has all permissions to every object in Trust Protection Platform.

Enter the user name and password. Password requirements are show on the screen. The password will be validated locally to verify it meets complexity requirements.

Verify the password, then click **Next**.

11. On the **Message Bus** tab, select whether or not you want to use a TLS-encrypted connection for the Message Bus (the MQTT broker used to communicate between servers in the cluster). The default is to use TLS.

    We recommend using the IANA registered ports for MQTT: port 8883 for TLS, or port 1883 for unencrypted.

    If you plan to use an external MQTT broker, click Central MQTT broker, then provide the URL to the service, and authentication information.

    For more details on Message Bus and its configuration, see "Working with Message Bus" on page 412.

    If you don't know what to enter here, you can likely accept the default values.

    Continue to the next tab by clicking **Next**.

12. On the **Algorithms** tab, you see the default algorithms available for global use with Venafi Platform. Click **Modify...** to edit the list. The table on the left is the list of algorithms supported by Venafi Platform that haven't been added to the approved list. The table on the right is a list of algorithms you want to be available globally for your organization. (You can further restrict algorithm use by policy, if you want settings to not apply globally.) To enable an algorithm, move it from the left table to the right table using the arrows.

    For details on configuring the default algorithms, see "About default algorithm configuration" on page 573. For a comprehensive list of supported algorithms, see "Algorithm types supported by Venafi Platform" on page 572.

    > **NOTE** If you are using an answer file that already includes supported algorithms, this tab won't let you adjust what is listed in the answer file. You can modify the supported algorithms after you finish the upgrade by going to Venafi Configuration Console (VCC), and clicking **Configure Allowed Algorithms**. For detailed steps, see "Configuring allowed algorithms" on page 574.

13. On the **Event Logging** tab, determine if you want this server to process log events.

    At least two Venafi servers needs to have event logging enabled. If event logging is configured on two different servers, you can leave this check box cleared.

Venafi recommends you define a retention period to control growth of the database. Trust Protection Platform will periodically automatically delete logs older than the specified number of days.

Click **Next.**

14. On the **Environment** tab enter the required information.

    Enter your organization name, and select the deployment type for the server, then click **Next**.

    Your organization name and deployment type are used in Venafi reports, and may be used in the future in other ways to enhance your product experience.

15. On the **Customer Experience** tab, review the information on how data is collected.

    NOTE Participation in the Customer Experience Improvement Project is required for all customers, enabling Venafi to gather license utilization and product usage telemetry. This does not include any personally-identifiable data. Read more about our data collection policy in the "Venafi Data Privacy Policy for Venafi Trust Protection Platform™" on page 987.

    Click **Next.**

16. On the **Save Configuration** tab, do the following:

    - Determine the location where the configuration progress and errors will be logged. If there is a problem with the configuration of the Venafi database, this file will show you where the error occurred, which will help Venafi Customer Support troubleshoot your issue more quickly and efficiently.
    - Specify whether Venafi Platform services should be started immediately upon completion of configuration.
    - We recommend you save your configuration as an answer file if this configuration is different than an answer file you have previously created. An answer file simplifies the process of upgrading Trust Protection Platform, reinstalling Trust Protection Platform, or installing more than one Trust Protection Platform server, connecting to the same database.
        - If you create an answer file, it is recommended that you encrypt your answer file with a password. An unencrypted answer file is a plain text XML file that contains information like your master admin user name and password, your database connection credentials, your software encryption key, and all other configuration settings.
        - If you are just completing the wizard to create an answer file, select the appropriate option. The wizard will save the answer file and will close when you click the **Finish** button.

17. Click **Finish**.

Venafi Platform will save the new configuration as an answer file in the specified location. When the answer file has been saved, click **Close**.

Configuring allowed algorithms

Venafi Platform supports many algorithms[1]. As a system administrator, you can define which algorithms your organization can track and use at the platform level, and set their priority. Policies can further restrict allowed algorithms, if needed.

By default, Venafi Platform has enabled all but the most insecure algorithms. When your administrator installed Venafi Platform, they had the option to change those default settings. If you find they need further refinement, a system administrator can make future changes in Venafi Configuration Console (VCC).

To configure allowed algorithms in VCC

1. In Venafi Configuration Console, under the root node, go to the **Actions** panel and click **Configure Allowed Algorithms**.
2. If prompted, enter the local master administrator credentials.
3. In the **Default Algorithm Configuration** window, adjust the allowed algorithms:
    - Use the left and right arrows to add or remove algorithms.
    - Use the up and down arrows to change the priority of allowed algorithms.
4. Click **Apply** to save your changes.

For additional information, see "About default algorithm configuration" on page 573.

Attention Required

The **Attention Required** node in Venafi Configuration Console provides a summary of issues with your Trust Protection Platform configuration that may need your attention. Each issue description provides guidance on how to resolve the issue. For select issues, you can click **Fix** in the upper right corner of the issue description to be taken directly to the location in Venafi Configuration Console where you can address that issue.

---

[1]For a comprehensive list, see "Algorithm types supported by Venafi Platform" on page 572.

Replacing the Venafi Operational Certificate (VOC) with your own CA-signed certificate

You should replace the Venafi Operational Certificate (VOC) that secures web services and the Trust Protection Platform log server with your own CA-signed certificate. However, replacing a VOC is slightly different than replacing other certificates. The Venafi IIS web site and the Trust Protection Platform Log server place certificates differently. Therefore, device and application objects are not required in order to place certificates. To ensure that you keep both the web services and the log server secure, refer to the following procedure.

To replace the VOC

1. From the Platform menu bar, click Policy Tree.
2. On the **Policy** tree, expand the **Venafi Operational Certificate** folder and select the VOC certificate.
3. On the **Settings** tab, clear the **Processing Disabled** check box.
4. In the **Management Type** field, select **Enrollment**.
5. If necessary, update the **Common Name** with the Fully Qualified Domain Name (FQDN) of the Trust Protection Platform server.
6. Select an existing **CA Template**. If none apply, create a new Certificate Authority (CA) template. For more information, see Managing certificate authority (CA) templates in the *Certificate Authority and Hosting Platform Integration Guide*.
7. Update any other fields as necessary, and then click **Save**.
8. In the **Platforms** tree, select your Trust Protection Platform engine.
9. On the **Settings** tab, assign the VOC **Certificate**, and then click **Save**.
10. (Optional) If you want the VOC to apply to more than one Trust Protection Platform server, repeat these steps for assigning the VOC to each server.
11. When the VOC certificate enrollment completes, navigate back to the **Policy** tree, expand the **Venafi Operational Certificate** folder, and then select the VOC certificate.
12. Click **Renew Now**.
13. After processing for the certificate completes, perform an IIS Reset on each server to enable the certificate to take effect immediately, or alternatively, the system will automatically provision the certificate at midnight (server time).

> **NOTE** To ensure any Server Agents have the opportunity to download the new trust bundle, any valid CA issue certificate will not be replaced by the system until two days prior to expiration.

Supporting new Server Agent installation *after* replacing your VOC

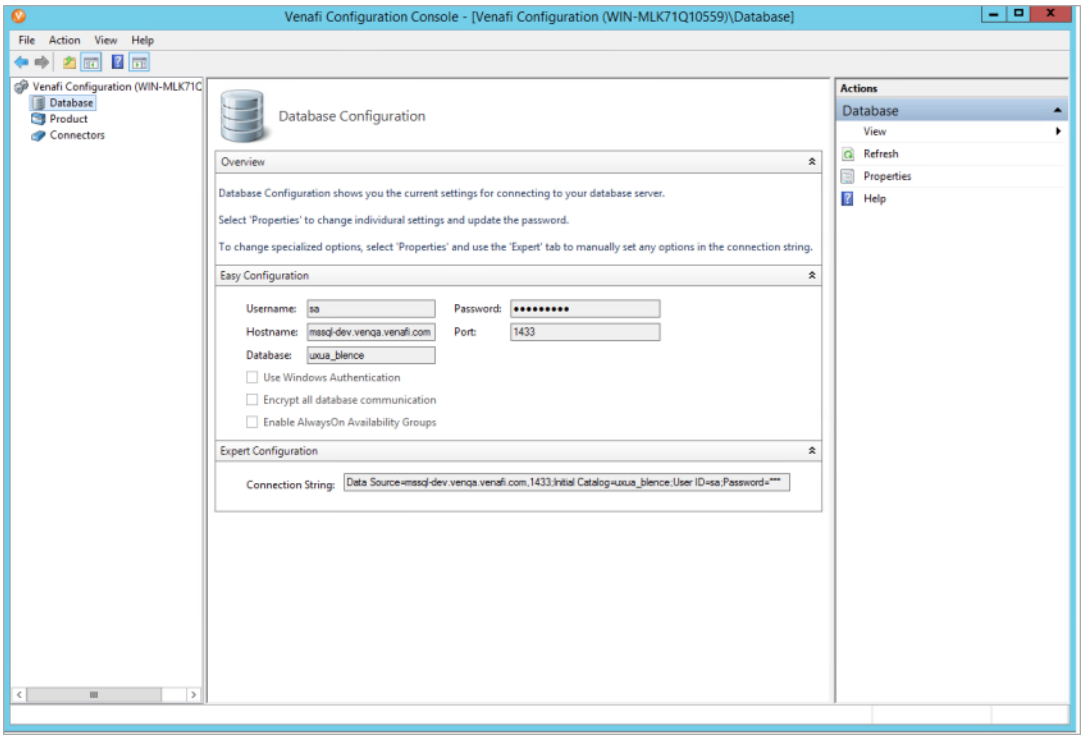
If the Server Agent will be installed in your Trust Protection Platform environment *after* the VOC has been replaced, copy the complete chain of the trusted certificate in the Roots tree. Then, update the **Agents should trust these additional issuers when reporting home** field with the new chain.

> **IMPORTANT** Certificates must be formatted using PEM (Base64 OpenSSL).

For more information about the Server Agent, refer to the *Server Agent Installation and Configuration Guide*.

Database configuration

The Venafi Configuration Console allows you to view and update the database connection for Trust Protection Platform.



Overview

The middle panel has the following sections:

- **Overview.** A description of the Database Configuration node.
- **Easy Configuration.** A display of the current database settings.
- **Expert Configuration.** Another representation of the database settings represented in a connection string.

Actions

The available actions for the database node are:

- **Refresh.** Allows you to refresh the database connection information.
- **Properties.** Allows you to change all the current database connection settings.

> **TIP** Each Venafi Trust Protection Platform server can use different database authentication credentials, allowing, for example, one server to connect using database credentials, and another server using Windows Authentication. The settings to the database in the Venafi Configuration Console affect only this application server's connection to the database.

Obtaining the SQL database connection string

The connection to the Trust Protection Platform database is stored as a connection string, and can be found in the Venafi Configuration Console. You may need this connection string if you want to do an advanced installation of Trust Protection Platform, or if you need to script an automatic credential change via the command line.

To obtain the SQL database connection string

1. On the Venafi server where Trust Protection Platform is installed, open Venafi Configuration Console.
2. Open the **Database** node.
3. In the Actions panel, click **Properties**.
4. If necessary, provide your Trust Protection Platform administrative credentials.
5. Click the Expert tab.

   The connection string shows you everything in the connection string except for the password.

   > **TIP** The password is not shown for security purposes.

6. Add the password to the string using the following format:

```
"-sqlconfig:<SQL string from Venafi Configuration Console>;Password=<Password>"
```

For example, if you have the SQL string:

```
Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbuser
```

and the password

```
S0m3thing-Compl3x!
```

Then the entire connection string would be:

```
TppConfiguration.exe -sqlconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbuser;Password=S0m3thing-Compl3x!"
```

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

Database Connection Repair

If the database can't be accessed when trying to run Venafi Configuration Console, the Database Connection Repair wizard will be shown.

If the database server is experiencing temporary downtime, Trust Protection Platform will resume working correctly when connectivity is restored. However, if the database connection information changes, you will need to repair the database connection.

To repair the database connection

1. On the application sever, open the **Venafi Configuration Console**.

   If the Configuration Console opens, the application server was able to communicate with the database, and you do not need to continue.

   If the application server was not able to communicate with the database, the Database Connection Repair wizard opens.

2. Read the information in the Database Connection Repair window, then click **Next**.

3. Update the database connection information, then click **Finish**.

- If the application server was able to connect using the updated information, the wizard will show that installation is complete, and you can click **Close**.
- If the application server was not able to connect using the updated information, the wizard will show a connection error. Correct any errors in the database settings, and click **Finish**.

To repair the database connection from the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-dboconfig` switch. The format is:

   ```
   TppConfiguration.exe "-dboconfig:<cfg>"
   ```

   For example:

   ```
   TppConfiguration.exe -dboconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOwnerUser;Password=S0me\"thing-Complex!"
   ```

   To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

To learn more about the TPPConfiguration utility, see "Using the TppConfiguration command line tool" on page 511.

Automatic credential rotation options

Trust Protection Platform provides the ability to rotate important system credentials using user-provided scripts via a command line interface (CLI). This means if you have an external system that rotates these credentials, you can write a script that will automatically change the connection information for Trust

Protection Platform automatically.

Credentials you can script for rotation:

- HSM connection pin
- Trust Protection Platform database connection password
- Identity provider. For more information, see "Updating an identity provider connection password" on page 748.

To reset the HSM connection pin using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-hsmpin` switch. For example:

   ```
   TppConfiguration.exe -hsmpin:<pin>
   ```

   NOTE If you don't include the PIN, the system will prompt you for the PIN in the next step.

   IMPORTANT The command line process does not validate the HSM PIN or database connection string. If you provide invalid data, you will not get a warning message. If you want to validate the data, use the Venafi Configuration Console interface, which does validate both the HSM pin and the database connection string.

   NOTE This utility is not designed to move your Venafi server from one database to another. It is intended only for changing credentials and scripting credential changes.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

For more information on using the command line to perform actions in Trust Protection Platform, see Configure the product from the command line in the Installation and Upgrade Guide.

To reset the Trust Protection Platform database owner account connection password using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-dboconfig` switch. The format is:

   ```
   TppConfiguration.exe "-dboconfig:<cfg>"
   ```

   For example:

   ```
   TppConfiguration.exe -dboconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOwnerUser;Password=S0me\"thing-Complex!"
   ```

   To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.

4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

To reset the Trust Protection Platform operational database account connection password using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-sqlconfig` switch. The format is:

```
TppConfiguration.exe "-sqlconfig:<cfg>"
```

For example:

```
TppConfiguration.exe -sqlconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOperationUser;Password=S0me\"thing-Complex!"
```

To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

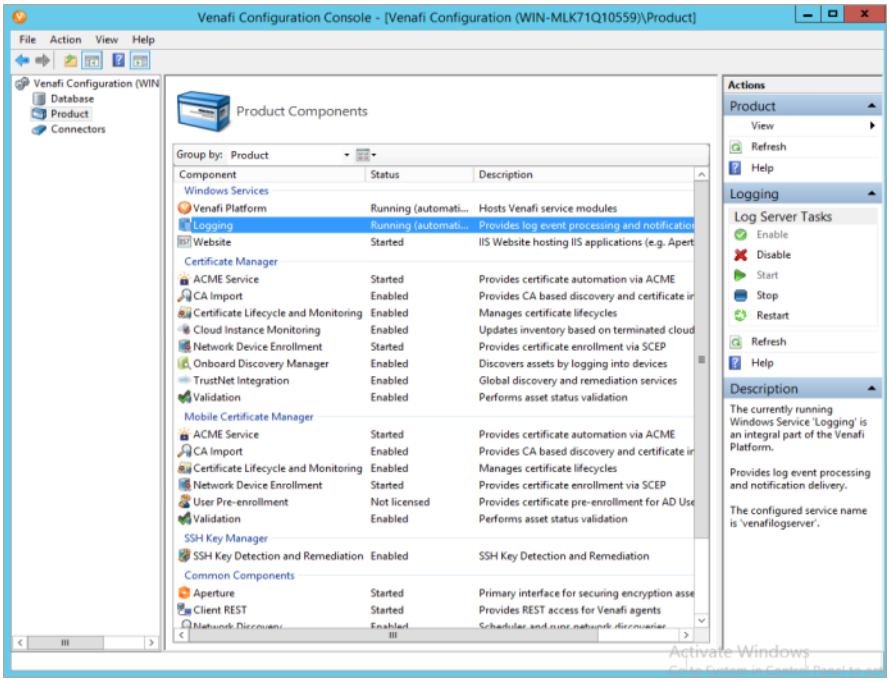
IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

For more information about the TPPConfiguration utility, see "Using the TppConfiguration command line tool" on page 511.

Product configuration

The Venafi Configuration Console (VCC) lets you manage the components that are enabled for the Venafi platform.

The features shown in the Product Components panel represent what is configured for a specific instance of Venafi Trust Protection Platform. Changes made to this panel only affect this specific server (if you have multiple servers in your cluster).



The center panel shows a list of Venafi product components and Windows services, and shows you the status for each item. You can start and stop Windows services, and control IIS Applications from this central location.

Click an item to see the actions available for that item.

For a list of Windows services available in Trust Protection Platform, see "Venafi Windows services" on the next page.

For a list of components available in Trust Protection Platform, see "Trust Protection Platform components" on page 843

Available actions

Depending on the item you select, there are several potential actions you might be able to perform.

The Descriptions section provides important details about the selected item including product component information, object name for the service module, and licensing information, if applicable.

These potential actions and when they are available are represented in the following table.

Action	IIS Applications	Windows Services	Venafi Service Modules
Start	X	X	
Stop	X	X	
Restart		X	
Recycle	X		
Remove	X		
Enable		X (Logging Only)	X
Disable		X (Logging Only)	X
Create	X		

For products that aren't licensed, no actions are available.

Venafi Windows services

The following is a list of modules that are available for selection in Venafi Configuration Console. Any module that is not selected during installation can be enabled later in the configuration console.

Some components can't be added to your system. For example, if IIS is not installed, or if you don't have a valid license for a specific product, related components won't be available.

Service	Description
Venafi Platform	This service hosts the Venafi service modules. This service is required for all Venafi products.
Logging	This service provides log event processing and notification delivery. It is not required to be running, however we recommend that at least one server in the cluster of Venafi servers has logging enabled and running.

Service	Description
API Host	This service is a WCF self-hosted web service used to run the Code Signing and Venafi Event Viewer MMC snap-ins on the Trust Protection Platform server. This service allows snap-ins run on the server even if IIS is not installed. It listens on port 689 and accepts requests only from localhost, to allow those snap-ins to perform their functions. By default, it closes after 10 minutes of inactivity.
Website	This is the IIS server. It is located in the Venafi Configuration Console to easily enable you to stop, start, and restart IIS without having to leave the Venafi Configuration Console. IIS must be running on all Venafi servers.
Enrollment over Secure Transport Service	This service provides certificate enrollment capability for devices via the Enrollment over Secure Transport (EST) protocol. For more information, see Configuring EST support on Trust Protection Platform.

Trust Protection Platform components

The following is a list of components that are available for selection in Venafi Configuration Console. Any component that is not selected during installation can be enabled later in the configuration console.

Some components can't be added to your system. For example, if IIS is not installed, or if you don't have a valid license for a specific product, related components won't be available.

Component	Answer file key	Products	Description
ACME Service	Acme	TLS Protect, Client Protect	Provides certificate automation via an Automated Certificate Management Environment (ACME). An HTTPS server is set up and configured to automatically obtain a browser-trusted certificate without any human intervention. A certificate management agent runs on the web server. **IMPORTANT** Venafi's implementation of the ACME protocol was designed and tested for use with the following clients: *certbot*, *win-acme*, and *acme.sh*. If you're using a different client, you might encounter limitations. For example, your alternate ACME client might use portions of the ACME protocol that aren't supported by Venafi's integration with the certbot and win-acme clients.
Authentication Server	AuthServer	Platform	Provides authentication for REST access for web components.
Automatic Layout Manager	AutoLayout	Platform	Enables Placement Job feature, allowing you to reconcile duplicates and organize certificates and devices in folders based on placement rules. If this feature is installed during installation of Venafi Trust Protection Platform, it can be enabled or disabled either in the Venafi Configuration Console, or in Policy Tree on the Platforms tree.

Component	Answer file key	Products	Description
			If you have multiple servers in your cluster, you may want to enable this feature on some, but not all, of the servers in the cluster for performance reasons. That would enable one server to be running the placement jobs feature without impacting the performance of other servers in the cluster.
Bulk Provisioning Manager	BulkProvisioning	TLS Protect	Provisions keys and certificates to one or more devices simultaneously.
CA Import	CAImport	TLS Protect, Client Protect	Automatically imports certificates from supported Certificate Authorities.
Certificate Lifecycle and Monitoring	Certificates	TLS Protect, Client Protect, CodeSign Protect	Provides certificate lifecycle management. Responsible for certificate-related tasks such as expiration notifications, issuance, renewal and revocation, and for provisioning of certificates to devices.
Certificate Revocation Monitoring	Revocation	TLS Protect, Client Protect	Provides the ability for Trust Protection Platform to provide CRL Distribution Point monitoring. Monitors the revocation status of all certificates in inventory at least daily. Allows you to do an on-demand revocation check for an individual certificate in either Aperture or Policy Tree. Monitors OCSP and CDP endpoint validity. This component does not control your ability to revoke certificates; this component adds the ability to monitor for revocations and to monitor CDP and OCSP endpoints.

Component	Answer file key	Products	Description
			IMPORTANT Certificate Revocation and CDP Monitoring is a feature that must be enabled when you install Trust Protection Platform in the Venafi Configuration Console. This module is *disabled* by default if you are upgrading from a version of Trust Protection Platform prior to 19.2. You will need to enable it manually on at least one engine if you want to do revocation checking and CDP monitoring. When you enable this module on multiple engines, all must have equal access to all CDP and OCSP endpoints. If a particular engine does not have the same network access as other engines, then the service module should be disabled on that engine with restricted access. If you see sporadic network access or "unable to connect" statuses for your CDP or OCSP endpoints (either in the Roots tree, or in the logs), it is likely that one of your engines does not have access to reach those endpoints. CDP Monitoring and Revocation Checking does *not* honor engine partitioning in the Policy tree.
Client REST	Client	Platform	Enables communication between agents and Trust Protection Platform.

Component	Answer file key	Products	Description
Code Signing Client Distribution	ClientDistribution	CodeSign Protect	Enables a web page that provides helpful scripting information and links for downloading CodeSign Protect clients. You can access the page by adding `/csc` to your Trust Protection Platform URL, such as: `https://TPP-Server-Name/csc` For more information, see Using the CodeSign Protect Client Downloads page.
Code Signing Key Server	KeyServer	CodeSign Protect	Provides functionality to set up a JWK key server and a GPG key server to store public keys and make them publicly available through a RESTful HTTP request. For more information, see GPG public key server.
Enrollment over Secure Transport Service	EstService	TLS Protect, Client Protect	This service provides certificate enrollment capability for devices via the Enrollment over Secure Transport (EST) protocol. For more information on EST, see Certificate enrollment via EST protocol.
HSM Backend	HsmBackend	CodeSign Protect	Provides virtual HSM capability within Trust Protection Platform for code signing. This allows Venafi CodeSign Protect clients to request signing operations using private code signing keys that are managed by Trust Protection Platform.

Component	Answer file key	Products	Description
Key Lifecycle and Monitoring	KeyManager	CodeSign Protect	Provides key lifecycle management. Responsible for tasks such creating new keys and monitoring key expiration. This component is required for GPG and .NET CodeSign Protect Environments, as well as for SSH Protect.
Kubernetes Discovery Manager	JSSDiscovery	TLS Protect	Provides a way to monitor TLS certificates used on clusters managed by Venafi TLS Protect for Kubernetes. With the Kubernetes discovery feature, administrators can create new discovery jobs which import certificates from all Kubernetes clusters registered to Venafi TLS Protect for Kubernetes.
Network Device Enrollment	Scep	TLS Protect, Client Protect	Enables devices to use the SCEP protocol to request certificates from Trust Protection Platform. You would want to enable this feature if you have SCEP-enabled devices or applications and you want those devices and applications to be able to get certificates directly from Trust Protection Platform. This feature is frequently used with mobile-device management solutions. For more information on configuring Network Device Enrollment, see Managing network device enrollment (NDE) of the *Venafi Trust Protection Platform Certificate Management Guide*.

Component	Answer file key	Products	Description
Network Discovery	Discovery	Platform	Runs the Network Discovery surveys configured in your system's Discovery objects. During a Network Discovery, the Discovery server scans designated IPv4 address ranges and ports to identify SSL certificates. For more information on discovering network certificates, see Discovering certificates and keys in the Venafi Administration Guide.
Object Monitoring	Monitoring	Platform	Monitors SSH key and credential objects for expiration and generates expiration notifications. For more information on logging and event notifications, see Notification and logging overview in the *Venafi Trust Protection Platform Administration Guide*.
Onboard Discovery Manager	OBDDiscovery	TLS Protect	Configuring onboard discovery jobs lets you automate the process of provisioning by adding devices to one or more specific policies. You then have control over the placement of discovered certificates without having to manually update jobs or reorganize certificates after they've been discovered.
Reporting	Reporting	Platform	Generates and distributes pre-defined and custom reports.
SSH Certificate Lifecycle and Monitoring	SSHCertificates	SSH Protect	Allow you to use SSH Protect to manage SSH Certificates.
SSH Key Detection and Remediation	SSH	SSH Protect	Secures and protect SSH keys and systems through discovery, reporting, policy enforcement, and remediation.

Component	Answer file key	Products	Description
Time Stamp Service	TimeStampService	CodeSign Protect	Provides an RFC 3161-compliant time stamping service for code signing. This service allows you to use either your own time stamping certificate or to specify a list of time stamping proxies. Once configured, you can then specify Trust Protection Platform as your time stamping server.
Validation	Validation	TLS Protect, Client Protect	Runs the network and onboard validation processes. Network validation verifies a certificate or key is installed on the target system, then determines if the correct certificate is being used. For more information on validating certificates and applications, see SSL/TLS network validation of the *Venafi Trust Protection Platform Certificate Management Guide*.

Component	Answer file key	Products	Description
Web Console	WebConsole	Platform	Web-based management interface. Installs both Policy Tree and Aperture. At least two Venafi servers needs to have Web Console enabled. If Web Console is configured on two different servers, you can disable this component. Server requirements for Web Console are outlined in System requirements for Venafi components.
Web SDK	WebSDK	Platform	Extend your custom environments by integrating them with Venafi solutions using the Venafi Web SDK code library. For more information, see About this guide in the *Trust Protection Platform Developer's Guide*.

Product Licenses

The **Licenses** node (under **Product** in the left panel) allows you to view the products that have been licensed, and add additional licenses as needed.

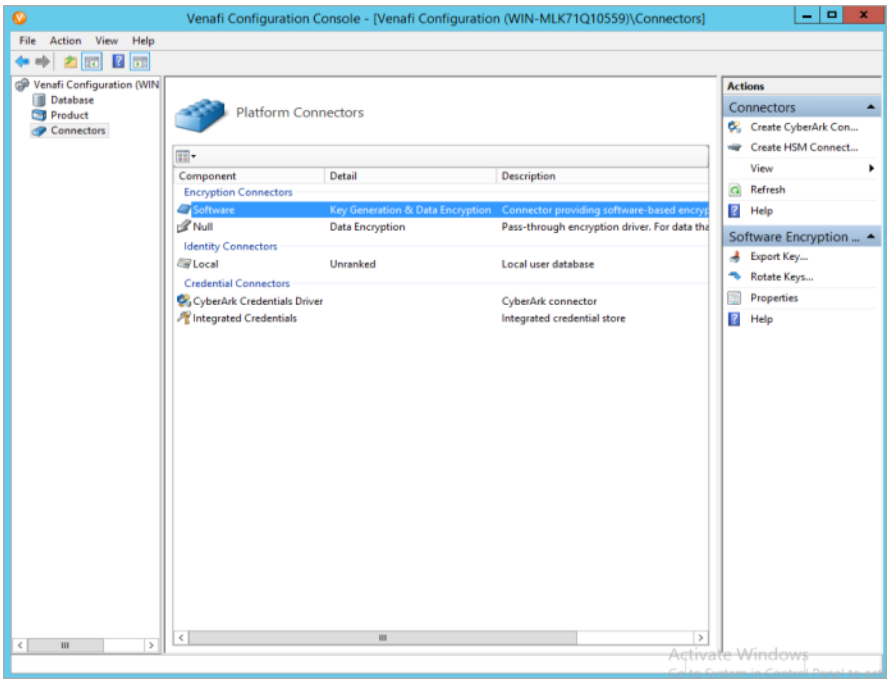
The **Product Licenses** window shows a list of all products with current licenses that have been installed on this Venafi Platform server. To add a license, use the following procedure.

To add a software license to your Venafi Trust Protection Platform

1. Open the Venafi Configuration Console and browse to the **Product** > **License** node.
2. In the Actions panel, click the product you want to enable.
3. If requested, provide the master administrator username and password to verify you have permission to make this change.
4. Close the Venafi Configuration Console and re-open it.

Connectors configuration

The Venafi Configuration Console Connectors node provides access to the various connectors that integrate with third-party hardware and software.



The categories of connectors are:

- Encryption Connectors

  The detail for each encryption connector shows how that particular connector is used. It will list one or more of the following:

  - **Data Encryption** - Data Encryption Key(s) stored on the HSM that are used to encrypt and decrypt key material
  - **Key Generation** - The HSM is used to generate the key pair. The key pair is then exported to Trust Protection Platform for storage. This feature requires Venafi Advanced Key Protect. For more information, see "Venafi Advanced Key Protect" on page 580.
  - **Key Storage** - The HSM is use to generate and store the key pair. The private key does not leave the HSM. Only applicable to CodeSign Protect. This feature requires Venafi Advanced Key Protect. For more information, see "Venafi Advanced Key Protect" on page 580 and Understanding CodeSign Protect.

- Identity Connectors

- Credential Connectors
- SMTP Default Connectors - The server configuration settings that allow Venafi Platform to send e-mail notifications through an SMTP server. For information, see "Setting up SMTP settings for outbound email connections" on page 435.

Click on a component to view the available actions for that component.

Actions Panel

You can create the following new connectors, or take one of the following actions:

- **HSM connector.** For information on creating an HSM connector, see "Creating a HSM connector" on page 562.
- **LDAP connector.** For information on creating an LDAP connector, see "Creating an LDAP connection" on page 650.
- **Active Directory connector**. For information on creating an Active Directory connector, see "Creating an Active Directory connection" on page 638.
- **CyperArk Connector.** For information on creating a CyberArk connector, see "Creating a CyberArk connector" on page 951.
- **Enable/Disable Venafi Advanced Key Protect.** Allows you to control your system's access to the Advanced Key Protect product. This feature requires a separate subscription. For more information, see "Enabling Venafi Advanced Key Protect" on page 590

Depending on the selected connector, you can take several actions including:

- **Export Key.** This is the action you take to export a copy of the system-generated (or manually entered) software key that encrypts the secrets stored in the Venafi Trust Protection Platform database. For more information see "Backing up the software encryption key" on page 554.
- **Rotate Key.** This action allows you to rotate an underlying encryption key used to encrypt secrets stored in the Venafi Trust Protection Platform database. For more information see "Rotate Secret Store encryption keys" on page 83.
- **Properties.** This action allows you to modify a connector's settings.

Backing up the software encryption key

When you installed and configured Venafi Trust Protection Platform, you had the option to enable either software or hardware encryption (or both). If you enabled software encryption, you need to back up the software encryption key to a secure location. The software key is critical to the functionality of Trust

Protection Platform. Without it, you cannot access data in the database. In the event of a system failure, you will need a copy of the encryption key to access your data. Additionally, if you want to install additional Trust Protection Platform servers, you will need the software key to install and configure those servers.

> **DID YOU KNOW?** How is the Venafi Trust Protection Platform software key used and why is it so important to back it up?
>
> Trust Protection Platform maintains all system information—that is, configuration settings, managed server and certificate information, archived certificates, and private keys—in a database. To secure this information, Trust Protection Platform uses an AES-256 encryption key—the software key—to encrypt the connection to the database.
>
> Depending on the encryption key selected in the object configuration, the objects themselves can be encrypted using the software key. The key is securely stored in the Windows registry.

For more information about why it's important to back up your data, see "Disaster recovery operations" in the Installation and Upgrade Guide.

To export the software key from Venafi Configuration Console

1. From the Venafi Trust Protection Platform server, open **Venafi Configuration Console**.
2. In the left panel, click **Connectors**.
3. In the center panel, click the **Software** component.
4. In the Actions panel on the right, click **Export Key...**
5. (Conditional) If requested, enter the Venafi Platform administrator user name and password.
6. Enter a password to encrypt the exported key.
7. Click **Browse** to select a location to export the key.
8. Click **Export**.

For more information, see "Venafi Configuration Console" on page 44 in the Administration Guide.

To export the software key from the command line

1. On the Venafi server, open a command line and browse to the Venafi installation directory.
2. Run the following command:

```
tppconfiguration.exe -keyexport:<file-path>
```

Rotate the System Protection Key

Rotating the System Protection Key will generate a new encryption key and re-encrypt all objects in the Trust Protection Platform database that are currently encrypted with the System Protection Key. When you rotate encryption keys, the system searches for all assets that are encrypted with the old key, decrypts them, encrypts them with the new key, and stores the newly encrypted value back in the database.

NOTE To learn more about how Trust Protection Platform uses the system protection key to protect assets, see "Managing system encryption keys" on page 545

Are you using the correct procedure?

There are two procedures with similar names, and it's important to verify which procedure you want.

- Rotate Secret Store keys
  - Secret Store keys are used to encrypt data in Secret Store, and focus on securing specific policy folders.
  - Different policy folders can be encrypted by different Secret Store keys.
  - Rotating Secret Store keys should be done regularly to maintain updated security.
  - During key rotation, the system searches for all assets that are encrypted with the old key, decrypts them, encrypts them with the new key, and stores the newly encrypted value back in the database.
  - This rotation can be initiated from the Venafi Configuration Console, and does not require any down time.
  - The procedure outlined below is NOT for rotating Secret Store keys. To rotate Secret Store keys, see "Rotate Secret Store encryption keys" on page 83
- Rotate System Protection key
  - The System Protection key encrypts everything stored in the Secret Store that isn't otherwise encrypted by a specific Secret Store key.
  - When you rotate the System Protection key, you create the new key, and then store it on the selected encryption connector.
  - The new key is encrypted using the current key and can be accessed by other Venafi Platform servers.
  - During the rotation process both the new and current keys remain active, allowing a seamless transition without downtime.
  - Once all objects have been re-encrypted with the new key, the current key is deleted from each Venafi Platform server.
  - The procedure below shows you how to rotate the System Protection key.

Learn more about how System Protection Key rotation works

- When System Protection Key rotation is initiated, Trust Protection Platform directs the creation of a new encryption key and stores that key on the encryption connector that you select.
- Trust Protection Platform encrypts the new key using the current key and stores it. The other Trust Protection Platform servers can then access the new key.
- Once it's confirmed that every server in the cluster has the new key, the key rotation begins. Objects encrypted with the current key will be re-encrypted with the new key.
- During key rotation, both the new key and the current key remain active on the Trust Protection Platform servers. This allows key rotation to happen in the background with no downtime.
- Once all objects have been re-encrypted with the new key, the current key is deleted from each Trust Protection Platform server.

Before you begin

- Make sure that you have a working HSM client on each server, and make sure that the HSM DLL file is in the same location on each server. To add a new HSM connector, see "Creating a HSM connector" on page 562.
- Make sure that you have a backup of your current key. If you're using a software key, follow the steps in "Backing up the software encryption key" on page 554. For keys stored on an HSM, verify that your key has been backed up in a recent backup of your HSM.
- The VPlatform service needs to be running to perform the rotation. There is no need to stop or restart services when performing a rotation. The encryption subsystem will dynamically reload when there is a change.
- When the key has been rotated, the change is replicated on all Venafi servers in the cluster within 5 minutes. For servers that Message Bus can connect to, this change is done near real-time.
- There is a rotation widget that appears in the System Dashboard in the web console when a rotation is in progress.

IMPORTANT After rotating your key, **you will need to replace your existing answer file with a new answer file that contains your updated key**. More information is provided after the steps in this procedure.

Steps for Key Rotation

1. From the Venafi Trust Protection Platform server, open **Venafi Configuration Console**.
2. In the left panel, click **Connectors**.
3. In the Actions panel on the right, click **Rotate TPP System Protection Key**.
4. In the **New Key Name** box, give this key a unique name.
5. From the **Connector** drop-down menu, select the location where you want the new System Protection Key to be stored.

   > **NOTE** If you select a connector other than your currently-used connector, the new key will be stored on the connector that you select.
   >
   > You can see what connector you are currently using in the Encryption tree of Trust Protection Platform. Open the Trust Protection Platform web interface by going to `https://<tpp-server-url>/aperture`. From the Platform menu bar, click **Policy Tree**. Then, in the drop-down menu near the top left corner, select **Encryption**.
   >
   > The **Default Key Generation** box shows your currently-used encryption connector, and the **Default Protection Key** box shows the name of the currently-used key.

6. From the **Rotate Keys On** drop-down menu, make a selection according to the following guidelines:
   - Selecting Any available server allows the first available Trust Protection Platform server in the cluster to perform the rotation. All other factors being equal, this is the recommended selection.
   - If you have one Trust Protection Platform with notably less latency to the database and to the HSM, we recommend selecting that server specifically.

   The keys will be rotated in the database by a single server, and all other servers will receive information about the new key.
7. If you are rotating your key from software to hardware, selecting **Disable software encryption** will ensure that the software key is no longer used.
8. Click **Rotate**.

   Depending on how many items there are to re-encrypt, this process may take a while. You can close the **Rotate System Protection Key** window (you can even close Venafi Configuration Console), and the rotation will continue to run in the background. You can check the status of the rotation by going to `https://<tpp-server-url>/aperture/platform/dashboard/tpp-services` and opening the Platform menu.

IMPORTANT Make sure to back up your new encryption key. If you've rotated a software key back into software, follow the steps in "Backing up the software encryption key" on page 554. If you've rotated the key to hardware, make sure you have backup procedures in place for your HSM.

IMPORTANT If you are using answer files for Trust Protection Platform installations, you must create a new answer file that contains your update key. Follow the steps in "Answer File wizard" on page 46.

You can see the status of the key rotation task by using the Rotation Widget in the System Dashboard (Aperture).

Log events

You can view log events related to rotating the System Protection Key in the Venafi Event Viewer. The Venafi Event Viewer can be opened either from the Venafi Configuration Console on the Trust Protection Platform server or by using the MMC Snap-in collection.

In Venafi Event Viewer, you can set up a custom view to see log events related to System Protection Key rotation.

1. To set up a custom view, open the Venafi Event Viewer and follow the steps in "Custom Views" on page 376.
2. In the **Event Sources** section, expand the **Venafi Secret Store** grouping, then click the checkbox next to the following:
    - **Secret Store - Key rotated**. Log event that indicates the encryption key for a given object was rotated.
    - **Secret Store - Keys rotated**. Log event that indicates the key rotation is complete.
    - **Secret Store - Server key rotation requested**. Log event that indicates the initiation of the key rotation.

Rotate Secret Store encryption keys

The Venafi Configuration Console provides the ability to rotate the encryption keys used to secure the information stored in Venafi Trust Protection Platform.

When you rotate the encryption keys, the system searches for all assets that are encrypted with the old key, decrypts them, encrypts them with the new key, and stores the newly encrypted value back in the database.

Are you using the correct procedure?

There are two procedures with similar names, and it's important to verify which procedure you want.

- Rotate Secret Store keys
  - Secret Store keys are used to encrypt data in Secret Store, and focus on securing specific policy folders.
  - Different policy folders can be encrypted by different Secret Store keys.
  - Rotating Secret Store keys should be done regularly to maintain updated security.
  - During key rotation, the system searches for all assets that are encrypted with the old key, decrypts them, encrypts them with the new key, and stores the newly encrypted value back in the database.
  - This rotation can be initiated from the Venafi Configuration Console, and does not require any down time.
  - The procedure outlined below shows you how to rotate Secret Store keys.
- Rotate System Protection key
  - The System Protection key encrypts everything stored in the Secret Store that isn't otherwise encrypted by a specific Secret Store key.
  - When you rotate the System Protection key, you create the new key, and then store it on the selected encryption connector.
  - The new key is encrypted using the current key and can be accessed by other Venafi Platform servers.
  - During the rotation process both the new and current keys remain active, allowing a seamless transition without downtime.
  - Once all objects have been re-encrypted with the new key, the current key is deleted from each Venafi Platform server.
  - The procedure below does NOT show you how to rotate the System Protection key. For information on rotating the System Protection key, see "Rotate the System Protection Key" on page 79.

Before you begin

- Make sure that all services will remain running until the task is completed. VPlatform needs to be running to perform the rotation. The encryption subsystem will dynamically reload when there is a change.
- This change is replicated across all Venafi Platform servers. When a server can be reached via Message Bus, the change is done in near-real time. If a server can't be reached via Message Bus, a ToDo will be created and all servers will be updated within about five minutes.
- You can see the status of the key rotation task by using the Rotation Widget in the System Dashboard on the web console.

To rotate encryption keys

1. From the Venafi Trust Protection Platform server, open **Venafi Configuration Console**.
2. In the left panel, click **Connectors**.
3. In the center panel, click the key that you want to rotate.
4. In the Actions panel on the right, click **Rotate Keys...**
5. (Conditional) If requested, enter the Venafi Platform administrator user name and password.
6. Select the old key from the list.
7. Select the new key from the list.
8. Click **Rotate**.

Depending on how many objects were encrypted with the old key, this process may take some time, however you can exit the Venafi Configuration Console as this task continues in the background.

Creating a HSM connector

After you have completed the necessary preconfiguration requirements, you can create the HSM connector in the Venafi Configuration Console. The HSM connector provides the information required to access encryption keys in Trust Protection Platform. Trust Protection Platform supports HSM connectors using the PKCS#11 standard using the Cryptoki API.

To create an HSM connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console**, and open the **Connectors** node.
2. In the Actions panel, click **Create HSM Connector**.
3. (Conditional) If requested, enter your Venafi Trust Protection Platform administration credentials.

4. Enter data into the fields, as described below.

Field	Description
Name	Name of the HSM connector. Use something descriptive so you can identify it later.
Cryptoki DLL Path	Trust Protection Platform requires access to the 64-bit version of Cryptoki DLL. For SafeNet Luna SA devices, this is the path to the `cryptoki.dll` file. For Entrust nShield Connect HSM devices, this is the path to the `cknfast.dll` file. After selecting the DLL, click **Load Slots**. Trust Protection Platform will query the HSM and return the available slots. **IMPORTANT** Trust Protection Platform requires the path to the DLL file to initialize the connection to the HSM device. This path will be used for all Trust Protection Platform servers in the cluster (connected to the same database). All servers in the cluster must have their DLL file in the same location.
Slot	Slot ID for the HSM partition where you want Trust Protection Platform to access the encryption keys. **NOTE** While slot numbers are listed in the drop-down list, Trust Protection Platform does not depend on slot numbers. Trust Protection Platform identifies HSM partitions by label first, and in the case that there are duplicate labels, it falls back to the serial number.
User Type	User type required to access the HSM keys on the designated partition (Slot ID). The designated User Type must have sufficient permissions to use the keys in the Encryption Driver's Permitted Keys list.
Pin	Pin, if one is required to access the HSM. If you use Entrust nShield token protection, leave the field empty. If you are setting up AWS CloudHSM, the pin must be in the following format: `<CU_user_name>:<password>`.

Field	Description
Permitted Keys	A list of keys that can be used for encryption and decryption of data by the Trust Protection Platform servers. The keys listed are the ones that can be used to encrypt data stored in the Trust Protection Platform Secret Store.
Allow Key Storage	Tells Trust Protection Platform whether this HSM can be used to generate and store new private keys associated with Code Signing certificates. **NOTE** This feature is available only for Venafi CodeSign Protect and requires Venafi Advanced Key Protect.
New Key (button)	If you want to generate a new AES 256-bit symmetric key on the HSM, click this button. A new key will be generated.

5. Click **Verify**.

These steps only create the connecter that exists between Venafi Platform and the HSM. You will need to use Policy Tree to enable the connector when you are ready. You will do that In **Policy Tree**, on the **Policy** root node. Click the **Certificate** tab. In the **Other Information** section, select your connector in the **Encryption Key** field.

WARNING! Don't change the Encryption Key field in the Policy Tree until the HSM configuration is installed on, and has been tested on every server in your cluster.

Once the HSM connector has been added and the connection has been verified, we recommend reviewing the post-installation steps.

Migrate existing HSM references to a new HSM

If you need to move existing keys to a different HSM or HSM partition, you can update the references to those keys in Trust Protection Platform to point to the new HSM.

This eliminates the need to recreate key references in Trust Protection Platform and allows your CodeSign Protect environments to continue to use the same keys, even though the keys themselves have moved to a new location.

EXAMPLE Many organizations use HSM partitions to manage access to keys stored on HSMs. Since CodeSign Protect provides its own access control to keys on HSMs, these organizations may no longer need separate HSM partitions for access management purposes. Using the HSM migration feature would allow keys to be moved to a consolidated HSM partition with minimal disruption to existing CodeSign Protect environments.

NOTE Migrating HSM reference applies only to private and public keys used in CodeSign Protect environments. References to keys used for data encryption can't be migrated.

Before you begin...

- Create a connector to the target HSM or HSM partition. Once complete, the **Connectors** view in Venafi Configuration Console should show both HSMs or HSM partitions—the one you're migrating from and the one you're migrating to.
- Copy every code signing key and key pair from the existing HSM to the target HSM. Follow your HSM vendor's documentation to copy the keys.

Follow these steps

1. In Venafi Configuration Console, go to the **Connectors** node, and then select the HSM partition you want to migrate key references off of.
2. In the **Actions** panel, click **Migrate references off this HSM**.

   A list of HSM references will open that shows the references that will be migrated.
3. Review the list and ensure that the target HSM has a copy of every key and key pair.
4. From the **Target HSM** drop-down, select your target HSM.

   If you don't see your Target HSM, cancel this procedure and go create an HSM connector to the target HSM.
5. Click **Migrate**.

Creating an LDAP connection

You can use the Venafi Configuration Console to create and view LDAP connections. A connection allows Trust Protection Platform to read User and Group data directly from an LDAP Identity Provider.

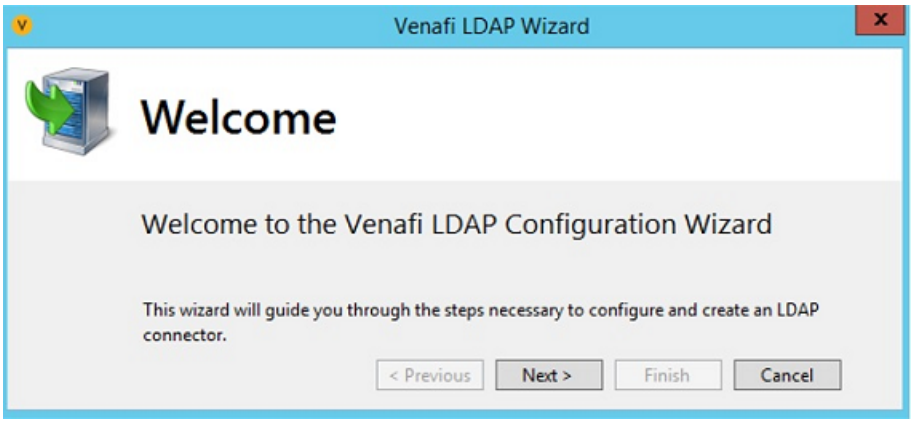
The Venafi LDAP Identity Wizard makes a connection from Trust Protection Platform to an LDAP Identity Provider. After the LDAP Identity Wizard completes, only the LDAP users and groups you specify can log in and use Trust Protection Platform based on assigned object permissions.

Trust Protection Platform supports LDAP identity object connections to providers using any of the following Internet protocols:

- IPv4 or IPv6-only connections
- IPv4 or IPv6 dual-stack (DS) connections

To create an LDAP connection

1. If you have not already done so, download and install the certificates required to establish an SSL connection with the LDAP server. If you are using the ODSEE vendor for LDAP, you can configure the LdapVendor.Oracle-DSee-11g.xml file to match your environment. For additional information about configuring for other vendors, contact Product Support.
2. Remote into the Trust Protection Platform server as a master administrator.
3. From the Windows **Start** menu, click **Venafi Configuration Console**.
4. In the left pane of VCC, click **Connectors**.
5. In the **Actions** pane, click **LDAP Connector**.
6. On the Welcome page, click **Next** and then log in with your credentials.



7. On the **Before You Begin** page, read the requirements, and then click **Next**.
8. On the **Connection Information** page, configure the connection between Trust Protection Platform and the LDAP Identity Provider, and then click **Next**.

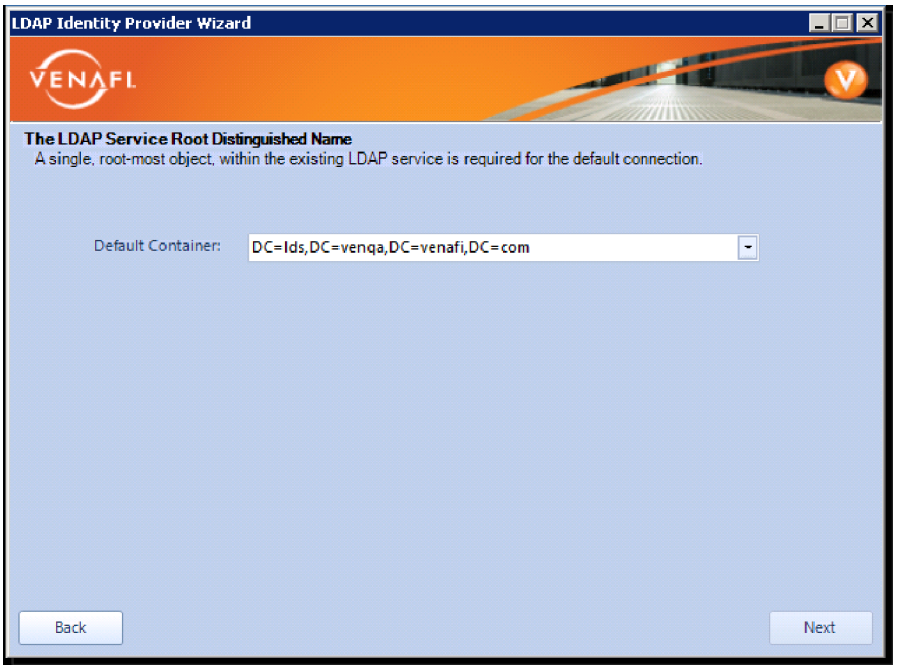
Parameter name	Description
Name / Address	A fully qualified DNS host name or IP address of the LDAP directory that requires connectivity to Trust Protection Platform.
Port	The port number for the connection between Trust Protection Platform and the LDAP Identity Provider. The default port is 636 for Lightweight Directory Access Protocol over TLS/SSL.
Timeout	The maximum number of seconds to search the provider for identity information.
Encryption	The kind of encryption to use between Trust Protection Platform and the LDAP Identity Provider: ◦ **No Encryption**: No encryption. (Not recommended). ◦ **Use SSL Encryption (ldaps://)**: The encryption is LDAP over Secure Socket Layer (SSL). ◦ **Use StartTLS Extension**: The extension to serialize secure and plain requests against the LDAP server on a single connection.
Disable certificate revocation check	(Optional) Bypass checking the revocation list to determine whether the encryption certificate is revoked.

Parameter name	Description
Allow anonymous binds	(Optional) Retrieve the initial binding context to the identity provider. If this option is cleared, the wizard connects via the user name and password that you supply on the next screen of the wizard. To retrieve the required naming contexts, the wizard anonymously binds *only* for the purpose of reading the rootDSE. All subsequent actions performed by the wizard will *always* perform a user bind.
Use 'Member Of' for group membership resolution	(Optional) Allow group membership resolution.
Disable user and group search validation by wizard	(Optional) Bypass validating the users and groups.

9. On the **Authentication Credentials** page, specify the required user Distinguished name (DN) and password of the Identity provider, and then click **Next**. For example, the User DN: cn=Admin,dc=odsee-qa,dc=venqa,dc=venafi,dc=com.

> **TIP** If you get an error that an LDAP vendor cannot be determined and that there's no available map was found, see the How To: Create new LDAP vendor map for new LDAP provider KB article.

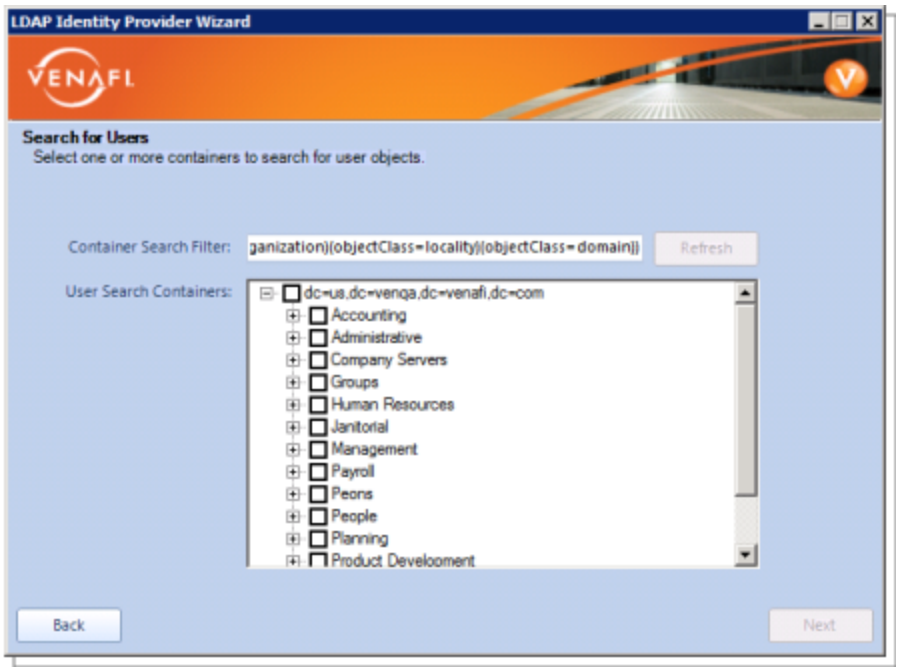
10. On the **Search Base** page, select the **Default container** from the list to search for user and group folders, and then click **Next**. No folders higher in the tree than this folder will be visible in future searches.



11. On the **User Search Root** page, type a folder search value in the **Container Search Filter** box, and then click **Refresh**. For example,
`(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=folder))`

    The results only list the User Classes list and the Group Search Expressions that are adaptable. The Remaining fields are read-only.

12. Select the user containers to include in the search. and then click **Next**.



13. On the **Group Search Root** page, do one (or both) of the following, and then click **Next**:
    a. (Optional) if you want your selections from the previous screen to be replicated in the **Group Search Containers** tree, select **Match User Search Containers**.

    b. (Optional) In the **Group Search Containers** tree, expand and select the groups to include in the search.

       The users and groups in the folders you select will be visible in the new LDAP connection that you are creating.

14. On the **Finalization** page, specify the following values as appropriate, and then click **Next**.

Parameter name	Description
Object Name	A name for your new LDAP Identity Provider object that appears in the Identity tree and in VCC. Choose a unique name that can help your administrators more easily recognize the providers.
Friendly Name	A name for internal use by Trust Protection Platform. Type a brief name with only alphanumeric characters and spaces. The **Friendly Name** can match the **Object Name**. However, the **Friendly Name** must be unique

Parameter name	Description
	for this object type in Trust Protection Platform.
Rank	The search order for this identity provider. If there are multiple identity providers, Trust Protection Platform searches for credentials starting with the lowest number first. In the case where there are identical names, such as Administrator, Trust Protection Platform finds the first instance. If the password is incorrect, no additional searches occur in the other providers.

What's next

1. Restart the Trust Protection Platform and Venafi Log Server services as well as any Web or Policy Tree sessions.
2. (Optional) If you want to log into Policy Tree as an LDAP user, restart the IIS server that is running on your Trust Protection Platform server. You can use the iisreset command to restart the IIS server.
3. Assign groups and users who need access to the new provider.
4. To review or update basic settings from VCC, click **Properties**.

Creating an Adaptable Credential connector

A connector is required if you want to connect Trust Protection Platform to a password vault. For detailed information about creating and using Adaptable Credentials, including prerequisites for configuration, see "Creating Adaptable Credentials" on page 921 in the *Trust Protection Platform Administration Guide*. Adaptable Credentials automate the retrieval of secrets from your third-party password vaults without compromising the security of your secrets.

The Adaptable Credential driver lets you create *username/password* and *password* credentials for retrieving their associated secrets that are stored by your third-party password vault. After creating your credentials, you assign them to certificates, applications and devices. During certificate enrollment and provisioning, their associated secrets are retrieved from the vault and are never stored in Trust Protection Platform.

To create an Adaptable Credential Connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console** (VCC), and then open the **Connectors** node.

2. In the **Actions** panel, click **Create Adaptable Credential Connector**.
3. (Conditional) If requested, enter your Trust Protection Platform administration credentials.
4. In the **Create Adaptable Credential Connector**, do the following:
5. In **Connector Name**, type a unique and descriptive name for your new connector.
6. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
7. Under **PowerShell Script**, select your custom Adaptable Credential PowerShell script.
8. (Conditional) Under **Connection details**, type the service address and credential needed to connect to your access management platform.
9. (Optional) Under **Identities with access to this connector**, select those users and groups who should be allowed to create Adaptable Credentials using your connector.
10. (Conditional) If this is the first time you're creating an Adaptable Credential connector, then restart the Policy Tree application pool on all Trust Protection Platform web servers.

Creating an Active Directory connection

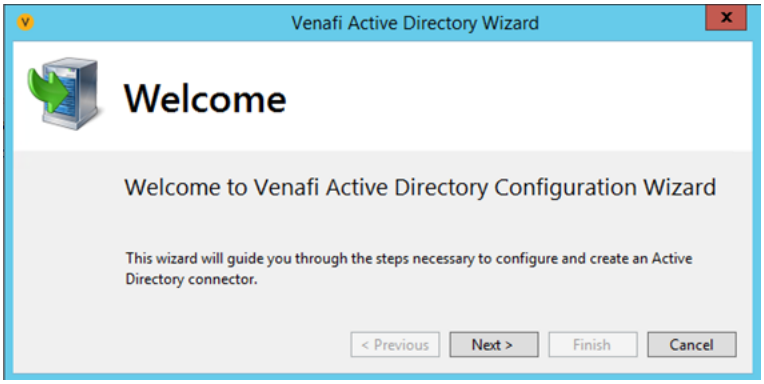
You can use Venafi Configuration Console to create and view Active Directory connections. Trust Protection Platform can connect to Active Directory via an IPv4 or IPv6 connection. You can create multiple Active Directory connections as necessary.

The Active Directory Connection integrates Trust Protection Platform with an Active Directory tree. The connection allows Trust Protection Platform to read User and Group data directly from Active Directory. So, you can log in as an external user, view external users and groups in the Identity tree, select external users or groups as object Contacts, and assign object permissions to external users and groups.

To create an Active Directory connection

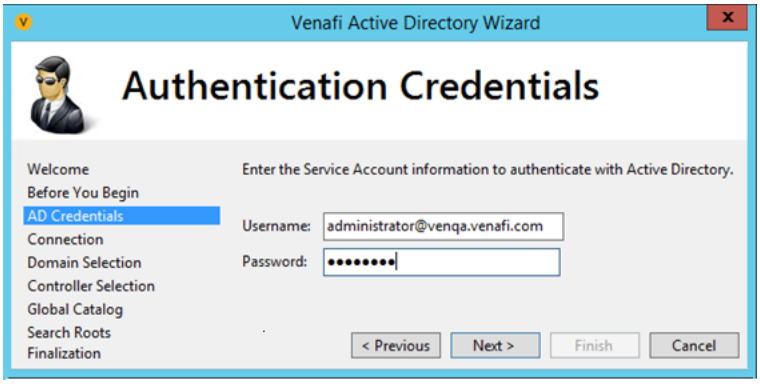
1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the left pane of VCC, click **Connectors**.
4. In the right **Actions** pane, Click **Active Directory Connector**.

5. If prompted, log in with your Trust Protection Platform local, master administrator credentials.
6. On the Welcome page, click **Next** and then log in with your credentials.



7. On the **Before You Begin** page, read the requirements. Be sure you know the AD root you want for the Root Selection step. Click **Next**.
8. On the **Authentication Credentials** page, type the credentials for the Active Directory service account, and then click **Next**.

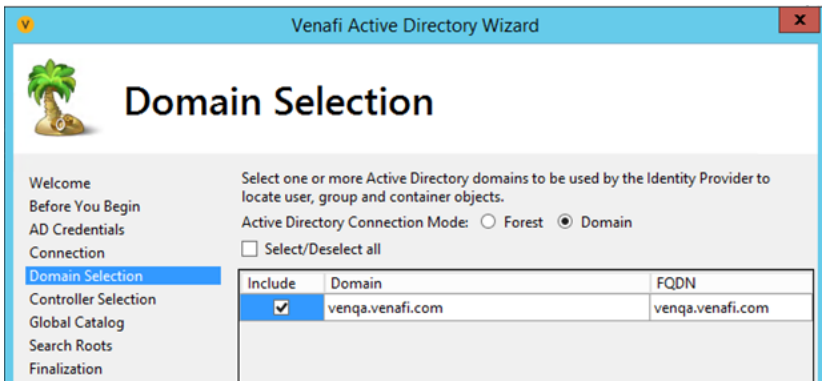
   The username must be in the User Principal Name (UPN) format. For more information, see "Requirements for creating an Active Directory connection" on page 636.



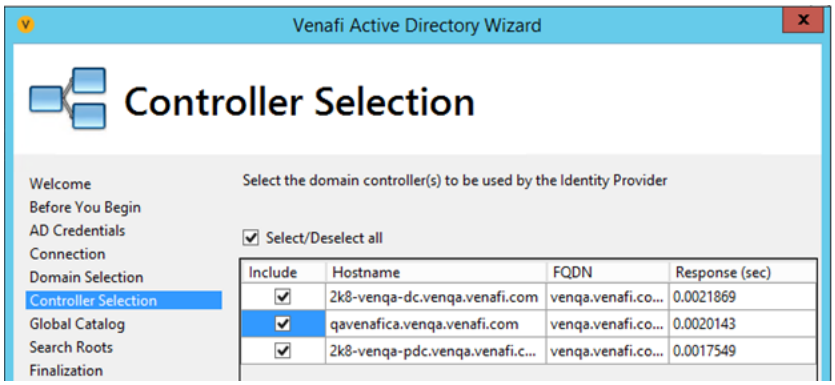
9. On the **Connection** page, enter the following information, and then click **Next**.

Parameter name	Description
Name	The Fully Qualified Domain Name (FQDN) of the AD host where Trust Protection Platform will connect and access Active Directory user domains, and then click **Next**. For example, host.example.co.
Connection	The managed AD directory: ◦ **Simple**: An unencrypted connection. ◦ **Secure**: An encrypted connection.
Concurrency	The number of processing threads to use for searching for users in the identity provider.
Choose Domains and Controllers Specific to this Platform	When selected, the settings you apply on the following screens will apply to this Venafi Platform server only. This allows you to have AD connectors in different security zones or segments in your network. When checked, the next box, "Disable Rediscovery for This Platform" will automatically be checked, and will be disabled, as it is required when you choose domains and controllers specific to this platform.
Disable Rediscovery for This Platform	If you are not choosing domains and controllers specific to a platform, leave this option **unselected** (which will leave rediscovery enabled) unless told to disable by Venafi Customer Support. This box will automatically become selected and disabled if the previous option, "Choose Domains and Controllers Specific to this Platform," is enabled.

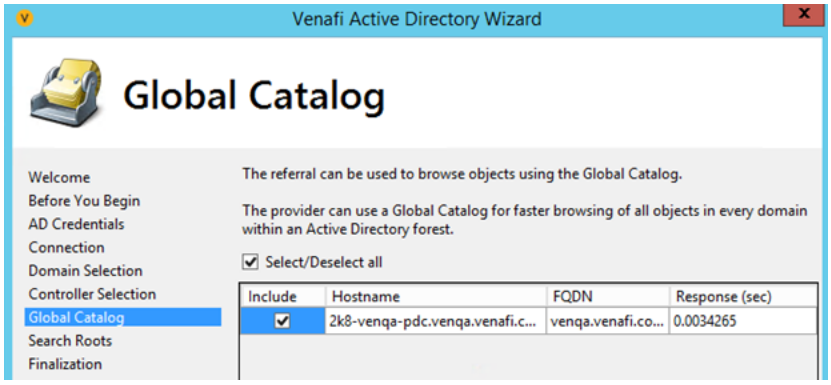
10. On the **Domain Selection** page, select the domains or forests to include, then click **Next**.



11. On the **Controller Selection** page, review the discovered domain controllers, and verify the correct controllers are selected for this network segment, then click **Next**.

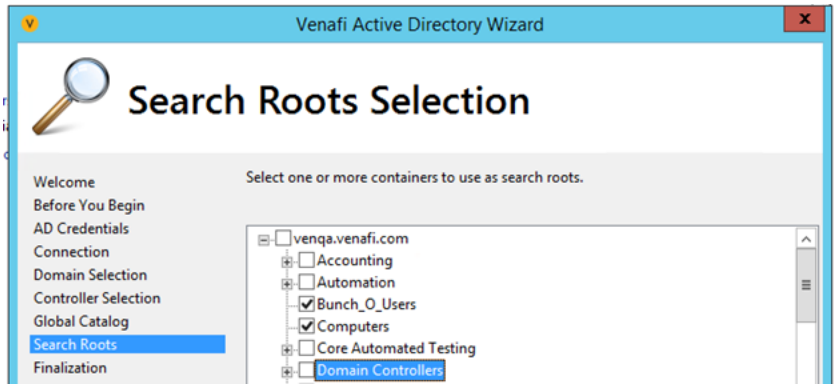


12. (Optional) On the Global Catalog page, review the discovered global catalogs, then click **Next**.



13. On the **Search Roots Selection** page, select the containers, and then click **Next**. If an error occurs, try the Common Name (CN) that appears in the error message as the container name.

Select nodes or containers where users connecting to Trust Protection Platform are found. If the users are in a node that is not selected, they will not be able to authenticate with Trust Protection Platform.



14. On the Finalization page, specify the following, and then click **Finish**:

Parameter name	Description
Object Name	Object Name that will appear in the Trust Protection Platform Identity tree.
Friendly Name	A friendly name for the AD connection. This is part of the Prefix for the identity connector. The complete Prefix will end up as AD+FriendlyName. This name should be easy to use and remember. A prefixed name, for example the AD+FriendlyName, is one of the allowed login formats.
Resolve Nested Groups	(Optional) The provider expands nested groups while processing notifications.
Rank	(Optional) The order the Identity connectors are searched when looking for users. For example, let's assume the username is Bob. If there is a username called Bob in the local identity system and the AD connector, we set the identity connector to tried first. Most likely, it is the AD connector, which means the AD connector needs to have a lower rank (highest priority). You would set the rank for the AD connector to **0** and the Local identity connector to **1**.

What's next

1. Restart the Trust Protection Platform and Venafi Log server.
2. Restart server services on all Trust Protection Platform servers.
3. Restart the IIS web server on all applicable Trust Protection Platform servers.
4. To review or update basic settings from VCC, click **Properties**.

Creating a CyberArk connector

A connector is required if you want to connect Trust Protection Platform to a CyberArk Enterprise Vault. For detailed information on CyberArk, including prerequisites for configuration, see "Using CyberArk with Trust Protection Platform" on page 944.

> Before you continue, set up CyberArk correctly. See "Getting CyberArk ready for integration with Trust Protection Platform" on page 944.

The CyberArk connector works with all Venafi Trust Protection Platform servers that connect to the same database.

To create a CyberArk connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console** and open the **Connectors** node.
2. In the **Actions** panel, click **Create CyberArk Connector**.
3. (Conditional) If requested, enter your Venafi Trust Protection Platform administration credentials.
4. In the **Create CyberArk Connector** window, complete the following fields:

Field	Description
Connector Name	Provide a name for the connector.
Description	Type any additional information that describes this connection. For example, the description could include the name of the server where the CyberArk Application Identity Manager (AIM) is installed.
Use Trust Protection Platform permissions model for credential access management	Select this option to skip all verification checks against the CyberArk PVWA and SCIM services. Identities with View access to the Connector object are allowed to manage CyberArk credential objects. If this option is not selected, user validation is done via CyberArk PVWA.
Privileged Account Security Web Services URI	Enter the location of your CyberArk Password Vault Web Access (PVWA) endpoint. For example: `https://webservices.host.com:1234/PasswordVault/WebServices` or `https://example.privilegecloud.cyberark.com/PasswordVault/`
Use Proxy	Check the Use Proxy box if you want the proxy to manage the CyberArk connection. This setting applies to the interaction between Trust Protection Platform, CyberArk Password Vault Web Access (PVWA), and Central Credential Provider. The Application Identity Manager (AIM/AAM), which is a standalone software component, requires additional Vault.ini configuration as detailed in the CyberArk Application Identity Manager Implementation Guide.
Web Service User	Type the user name you created for Trust Protection Platform to use when verifying the permissions a user has been granted to a CyberArk safe. **NOTE:** This is not applicable when Certificate (PKI) authentication method is selected for the Web Services Authentication Method

Field	Description
	NOTE: This is a service account. The account must have View safe members permission to all safes that the end users are allowed to retrieve secrets. Refer to Check permissions on safe members for more details.
Web Service Password	Type the password for the user you created for Trust Protection Platform to use to verify CyberArk safe permissions. **NOTE:** This is not applicable when Certificate (PKI) authentication method is selected for the Web Services Authentication Method
Service Account Authentication Method	Select the authentication method to use to authenticate to the vault. Supported methods include CyberArk (1st gen API), CyberArk (2nd gen API), LDAP (2nd gen), RADIUS (2nd gen), Windows (2nd gen), and Certificate (PKI). **NOTE:** When Certificate (PKI) authentication method is selected, you MUST specify the certificate credential in **WebAdmin** > **Credentials tree** > **Credential Drivers** > **CyberArk Connector** .
SCIM Server URI (optional)	If you have a configured CyberArk SCIM server, add the SCIM service address. For example: https://scimserver.example.com/CyberArk/scim/v2 The main scenario for which TPP uses the CyberArk SCIM is when the end user (CyberArk, LDAP, RADIUS or Windows) that is retrieving the account (secret) is not a direct member of a Safe but is a member of a CyberArk group. In this case SCIM Server URI, SCIM Server User and SCIM Server Password MUST be provided on the

Field	Description
	CyberArk connector of TPP (see the TPP setup for CyberArk when retrieving accounts section). The group itself MUST be a member of the Safe and MUST have **Retrieve accounts** or **Use accounts** permission to the Safe for the end user to successfully retrieve the account (secret) from the Safe.
SCIM Server User SCIM Server Password	Enter the SCIM server URI, user name and password so that Trust Protection Platform can authenticate to your SCIM server. This is a service account created by the CyberArk administrator for use by TPP. This user MUST be able to authenticate to the CyberArk SCIM server Following successful authentication, your CyberArk connector setup is complete. **DID YOU KNOW?** If you specify the correct URL, user name and password and authentication fails, then Trust Protection Platform attempts to authenticate with the CyberArk user name and password.
Password Retrieval Method	Select a method to use for password retrieval. ◦ If you select **Windows Credential Provider (AAM Agent)**, then select a version from **Windows Credential Provider Version**. ◦ If you select **Central Credential Provider**, then enter the **Central Credential Provider Web Service URL**. If you use Central Credential Provider, then you don't need to install the CyberArk AIM/AAM agent on a Trust Protection Platform server. To configure certificate-based authentication to

Field	Description
	Central Credential Provider see Configuring and editing the CyberArk Credentials driver in the Policy Tree **DID YOU KNOW?** You can find the installed version of the Windows AIM/AAM Agent using RDP to the machine where the AIM/AAM agent is installed. Then open **Programs and features** and search for the CyberArk AIM/AAM Agent installation in the list and check its version.
Windows Credential Provider Version	This option is only available when Windows Credential Provider (AIM/AAM Agent) is selected. Select the version of the Windows AIM/AAM agent. **DID YOU KNOW?** You can find the installed version of the Windows AIM/AAM Agent through RDP to the machine where the AIM/AAM Agent is installed. Then open **Programs and features**, and search for the CyberArk AIM/AAM Agent installation in the list to check its version.

5. Click **Create**.
6. Restart IIS.

You can see the new connector in the **Credential Connectors** section of the Venafi Configuration Console. You will also be able to see the connector, as well as the new server user credential that was created, in Policy Tree, in the Credentials tree.

NOTE Trust Protection Platform only supports one CyberArk connector. You cannot connect to multiple CyberArk vaults.

Enabling Venafi Advanced Key Protect

With Venafi Advanced Key Protect, you can use an HSM to generate keys and, in the case of CodeSign Protect, store private keys remotely. This is an optional add-on feature to Venafi Trust Protection Platform.

To enable or disable Advanced Key Protect

1. On the Venafi Trust Protection Platform server, open the Venafi Configuration Console, and click the Connectors node.
2. In the Actions panel, click **Enable Advanced Key Protect** (or **Disable Advanced Key Protect**).
3. Review the information in the dialog boxes and confirm the action.
4. Restart the IIS service by going to the **Product** node, and clicking on **Website**, and then clicking **Restart**.
5. Restart the Venafi Platform service by clicking on **Venafi Platform**, and then clicking **Restart**.
6. Restart the Logging service by clicking on **Logging**, and then clicking **Restart**.

The change is reflected on the License Report that is automatically submitted to Venafi. For information about the license report, see Venafi License Report.

Setting up SMTP settings for outbound email connections

Venafi Platform has powerful logging capabilities, with a variety of methods of delivery. After database logging, the most popular form of notifications is via email.

Venafi Platform will *not* be able to send email notifications for log channels or for the reporting service until you configure the outbound SMTP server settings, as described below.

The SMTP server settings you want to use may be the same for both log channels and the reporting service, however you need to set up both if you are using both features. Keeping the configurations separate allows you to use different email settings for the different purposes.

Configuring the SMTP Default Connectors for Log Channels and Reporting in VCC

1. In Venafi Configuration Console, open the **Connectors** node.
2. In the SMTP Default Connectors section, click the connector you want to configure.

- **Log Channels**. This connector controls the SMTP email configuration for all SMTP Log channels. For more information, see "Setting up notification channels" on page 439
- **Reporting**. This connector controls the SMTP email configuration for all Reporting service modules.

3. Click **Properties**.
4. If prompted, log in to Venafi Platform using an account with system administrator permissions.
5. Enter the SMTP Server information as outlined in the table below.

Field	Description
Host	Enter the SMTP host name or IP address. For example: `smtp.example.com` or `127.0.0.1`.
Port	Enter the port to use for the SMTP connection. The default port for SMTP connection is 25, which does *not* encrypt the connection. To use Secure TLS communication, you cannot use port 25. Here are the three standard SMTP ports: ◦ Port 25. (Default) This is a non-secure default SMTP port. ◦ Port 465. This port securely sends email via SMTP by SSL/TLS. ◦ Port 587. This is the successor port of port 465 and is often seen as the default transmission channel for secure SMTP connections. **About secure SMTP connections** Venafi uses SMTP Authentication for outbound email. We are investigating support for OAuth2, but the currently-implemented OAuth2 flows are created for client applications where the user can be periodically prompted for credentials (or MFA) to obtain a new grant. As a server application, Venafi requires an unattended authentication method. We strongly recommend you configure your SMTP to use Secure TLS communication on a supported port. The Microsoft Exchange team's solution for continued support is using High Volume Email (HVE) for Microsoft 365, Azure Communication Services for Email, or an Exchange Server on-premises in a hybrid configuration.

Field	Description
	For instructions on how to onboard to High Volume Email for Microsoft 365, see instructions from Microsoft at https://learn.microsoft.com/en-us/Exchange/mail-flow-best-practices/high-volume-mails-m365. This solution uses port 587 and authenticates to Office 365 using a HVE account username and password.
Sender E-mail	This is the e-mail address the recipient will see in the "From" field of their email message.
Use Secure TLS communication	This setting enables the email client and server to exchange messages using the Transport Layer Security (TLS) protocol, which encrypts the data and verifies the identity of and integrity of the parties involved.
Log event for each delivered message	When checked, Venafi Configuration Console will log an event for every email message it sends. This feature is useful to meet some organization's auditing requirements.
Lock settings [...]	When checked, individual SMTP channels or Reporting modules will not be able to override these settings. This is analogous to locking the policy setting.
Authenticate to SMTP Server	This setting requires the email client to provide a valid user name and password to the SMTP server before it can send or receive email messages. When selected, the following two fields become available.
Username	The username used to authenticate the SMTP connection to the email host.
Password	The password used to authenticate the SMTP connection to the email host.
Send Test E-mail	Click to test the connection to ensure Venafi Platform can send messages using these settings.

6. Click **OK**.

IMPORTANT Until SMTP outbound server settings are configured for the first time, SMTP channels are disabled. Do not attempt to send any logs to SMTP channels until you configure SMTP outbound server settings as described above.

The first time you configure an SMTP connection, the built-in SMTP channels automatically become enabled.

System Roles

The **System Roles** node allows you to view, assign, and delete several pre-defined roles including Master Administrator, Auditor, Access Management Administrator, Recycle Bin Administrator, Schema Administrator, and Code Signing Administrator.

> **NOTE** The **Code Signing Administrator** option appears only if you have licensed CodeSign Protect.

Viewing current role assignments

Click the **System Roles** node in Venafi Configuration Console, and the middle panel will display the users who are currently assigned to one (or more) of the system roles. If a user has more than one role, their identity appears once for each assigned role.

Using the **Group by** drop-down at the top of the list, you can sort the list either alphabetically or by type.

> **IMPORTANT** This list shows roles that have been assigned **directly to user identities or group identities.** Since users can inherit roles from the groups they belong to, a user may have a role, but not be listed here, if they are a member of a group that is assigned that role.

Assigning new role assignments

1. In the **Actions** panel, click the **Add** action for the role you want to add to a user or group..
2. Search for the user you want to assign, and click **Select**.

Removing current role assignments

1. From the administrators list, select the user whose administrator rights you want to remove.
2. In the **Actions** panel, click **Delete**. You will be prompted to confirm the rights removal.

About the Allow Team Creation role

There is one "role" that you cannot assign in VCC called *Allow Team Creation*. This is actually a grant and not a system role. You manage this grant in the Policy Tree. Locate the user or group in the Identities tree. For more information, see "Managing role and grant assignments in Policy Tree" on page 710.

Authentication configuration

The Authentication node of Venafi Configuration Console allows you to configure settings related to how users can authentication to Venafi Platform using a variety of popular Identity Providers, including:

- Okta
- Ping Identity (including PingFederate, PingOne for Customers, and PingOne for Enterprise)
- Azure
- ADFS

As of Venafi Platform version 25.1, there is only one authentication connector, which is SAML. We anticipate migrating other authentication types (such as Windows Authentication and Certificate authentication) from WebAdmin to the new Authentication node in a future release.

You can only configure one authentication connector. Venafi Platform does not support connecting multiple authentication connectors at the same time.

To configure SAML authentication for Venafi Platform, see "Prepare Venafi Platform for SAML SSO" on page 813.

Configure web console session timeout

The Authentication node is also where you configure the session timeout settings for the web console.

To configure session timeout settings

1. In the **Authentication** node of Venafi Configuration Console, click **Session Timeout Settings** in the **Actions** panel.
2. [Conditional] If required, enter your admin credentials.
3. Specify the timeout duration
4. Specify the timeout duration unit

   For example, you could specify *30 minutes* or *4 hours*.

   The timeout value must be between 15 minutes and 24 hours.
5. Click **OK**.

> **NOTE** This value will not be applied until you stop and restart the web server. You will need to restart all web servers in the cluster to propagate this change. This can be done in sequence to prevent (or minimize) downtime.

> **TIP** These settings will be retained when you upgrade to a new version of Venafi Platform.

Working with SAML for single sign-on (SSO)

Venafi Platform allows you to use modern single sign-on (SSO) identity providers (like Okta, Azure, Ping Identity, etc.) that use the SAML 2.0 standard. Using a third-party identity provider can greatly enhance your security posture. For example, they can simplify configuration of two-factor authentication (2FA), a protection against phishing threats and other password vulnerabilities.

Venafi Platform has long allowed you to use a variety of single sign-on methods like Windows authentication and certificate authentication. With the ability to connect to identity providers (IDP) via SAML, you have even more options for protecting your machine identity management system.

In this release of Venafi Platform, there are some items you should be aware of:

- When you import the identity provider SAML file, the associated certificate is automatically enrolled in TLS Protect at the *monitoring* level. A higher level of enrollment is not possible, since SAML certificates are not issued and imported like a normal certificate. To renew the SAML certificate you need an entirely new identity provider metadata file.
- Venafi Platform requires the entire SAML Response to be signed (but not encrypted, which is not supported). Some IDPs only sign the Assertion, so you may need to specify signing the entire Response.
- We do not support signed authentication requests.
- The default search expression will need to be changed, as documented in the phase one instructions.
- We do not currently support single log out (SLO), however, we do support a Logout URL, if your IDP allows you to log out by simply visiting a URL.
- We do not support forced log on.
- You can only configure one Authentication connector at a time. We don't support multiple connectors.
- While any SAML 2.0 IDP should work, we have tested with the following:
    - Active Directory
    - Azure
    - Okta
    - Ping
- The clock skew allowance is set to 180 seconds. The Venafi server and IDP server time can be off by 180 seconds and still sign in.

Configuration process

There are three high-level steps to configure SAML SSO for Venafi Platform.



Phase 1. Prepare Venafi Platform for SAML and obtain the Service Provider Metadata XML file. See the steps in "Prepare Venafi Platform for SAML SSO" on page 813.

Phase 2. Configure the Identity Provider and obtain the IDP Metadata XML file. The steps for phase two depend on your IDP. We've tested and outlined the following:

- ADFS
- Azure
- Okta
- Ping Federate
- Ping One

Phase 3. Configure SAML on your Venafi server. See the steps in "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

If you have questions, try reviewing "SAML troubleshooting tips" on page 835.

Technical implementation details

On the SAML signing certificate we verify:

- The certificate is not expired
- The certificate matches the certificate we have on file for the SAML profile
- The correct certificate was used to create the signature
- The signature is still valid (validity period hasn't expired and certificate has not been revoked).

The SAML Response must:

- Contain the `ID` attribute
- Contain the `version` attribute, and the version must be `2.0`

- The `InResponseTo` attribute must match TPP's authentication flow
- Have a signature on the response
- The `destination` must be entered, and must match the FQDN of the Venafi cluster
- `Status` must be present, and have a value of `Success`
- `Issuer` must be present, and must match the issuer on the SAML profile

The SAML Assertion must:

- Contain the `version` attribute, and the version must be `2.0`
- `Audience` attribute must equal the Venafi Platform service provider ID
- Contain a `Subject`
- `SubjectConfirmation` attribute must be present, and have the method of `bearer`
- If the assertion is signed, the signature must be valid (however, the assertion does not need to be signed)
- The `NotBefore` and `NotAfter` attributes in the Conditions are validated, respecting clock skew
- Contain the `Issuer`, which must match the issuer on the SAML profile
- Assertion `ID` must be present
- The `NotOnOrAfter` attribute must be present in the assertion

Prepare Venafi Platform for SAML SSO

Venafi Platform supports a number of popular SAML single sign-on (SSO) identity providers for modern SSO user authentication.

Configuring SAML single sign-on (SSO) is a multi-step process that involves getting your Venafi instance ready, configuring your identity provider, and then incorporating your identity provider's data in Venafi Configuration Console.

This topic is part of Phase One (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

Phase One of SAML SSO configuration can be broken down into the following processes:

1. Configure your FQDN in Venafi Platform's Platform tree so it knows what URL people are using to access its services. This is required because the signed SAML Response is linked to the FQDN, and if

this isn't configured properly, SSO won't work.

2. Ensure you have an LDAP or Active Directory (AD) connection to an identity directory that is connected to your SAML Identity Provider (IDP).
3. Configure the User Search Expression for you identity store (LDAP or AD). This step uniquely links users in your directory with users in Venafi Platform via a specific user identifier, like UPN.
4. Export your Venafi Service Provider Metadata XML file. This file (or the data it contains) will be required for phase two: configuring your IDP.

Each of these processes is described in the sections below.

Phase 1.1: Configure your FQDN

A secure SAML SSO process requires you provide the FQND (fully-qualified domain name) users enter to access Venafi Platform. Most organizations use multiple Venafi Platform servers to provide redundancy and load balancing. The server doesn't know the URL (of, for example, the load balancer) but the FQDN is required for secure communication between your Venafi server and the IDP. Use the following procedure to configure your FQDN in the web console.

To configure your FQDN in Venafi Platform

1. From the Platform menu bar, click Policy Tree.
2. Click the **Platforms** tree.

   You will be taken to the **Platforms** root, **Platforms** tab.
3. Click the **Engine** sub-tab.
4. In Trust Protection Platform **URL HostNames**, locate **Aperture (/Aperture)**, and enter the FQDN or IP address used to access Venafi Platform. The value you enter should match the FQDN found in the common name or DNS Subject Alternative Name of your CA-issued Venafi Operational Certificate so users don't encounter a certificate error.

   NOTE Do NOT include the protocol (`https://`), or the `/Aperture` directory. Just enter the FQDN itself. So, if your Aperture URL is `https://platform.venafi.com/Aperture`, you would enter:

   ```
   platform.venafi.com
   ```
5. Click **Save**.

Phase 1.2: Ensure you have connected Venafi Platform to AD or LDAP

In Venafi Platform version 25.1, there is no support for just-in-time account creation, so you need to have Venafi Platform accounts for all users who will be logging in via the SAML identity provider as Active Directory (AD) or LDAP users.

It is important that your users are queryable by the value put in the NameID parameter of the Subject section of the SAML assertion. For example:

- For AD users, if the SAML IDP is using the e-mail address of the authenticated user as the NameID, then the Venafi Platform AD identity provider User Search properties should be configured to customize the user lookup to the email address. For details on customizing the user lookup to the email address, see "Phase 1.3: Configure SAML user search expression" below.
- For LDAP users, if the SAML IDP is using the UPN (User Principle Name) of the authenticated user as the `NameID`, then the Venafi Platform LDAP identity driver User Search properties should be configured to add `userPrincipalName` (or whatever the corresponding attribute is in your LDAP directory) as described in "Phase 1.3: Configure SAML user search expression" below.

  Whatever the attribute is, you want to follow these guidelines:

  - The attribute is something that the SAML IDP can provide.
  - The attribute is something that Venafi Platform has access to and can query against.
  - The attribute uniquely identifies one (and only one) user. If more than one user is returned in the query, authentication will fail an ambiguity security check.

Regardless of the identity provider, you need to export Venafi Platform data that you will use to connect to the identity provider.

The steps you need to take to configure Active Directory are in "Creating an Active Directory connection" on page 638. Complete AD configuration information can be found in "Working with Active Directory" on page 636

The steps you need to take to configure LDAP are in "Creating an LDAP connection" on page 650. Complete LDAP configuration information can be found in "Working with LDAP and Oracle directory service" on page 648.

Phase 1.3: Configure SAML user search expression

When configuring a SAML-based identity provider configuration for logging in to Venafi Platform, you need to ensure the identity driver is configured to customize the user lookup to correctly and uniquely identify users.

You need to work with your identity management team to determine what type of unique identifier you are able to pass into the user assertion. We recommend using UPN, but you can use any unique attribute that is available to be put as the `Name ID` of the SAML assertion, and is available for query via your AD or LDAP connection.

To customize the user lookup in Venafi Configuration Console

1. Use Remote Desktop to connect to the Venafi Platform host machine, and open the **Venafi Configuration Console**.
2. Click the **Connectors** node.
3. Click the identity connector used by Active Directory.
4. In the actions panel, click **Properties**.
5. [Conditional] If necessary, log in to Venafi Platform as a master administrator.

   The next step depends on whether you are connecting with AD or LDAP.

   #### For Active Directory

   a. Click the **User Search** tab.

   b. Click **Use Custom Expression**.

   c. Change the value from:

   ```
   (&(ANR=$search$*)(objectCategory=$userclass$))
   ```

   to:

   ```
   (&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))
   ```

   Unless your IDP is *not* sending the UPN of the user within the `userID`, in which case you should enter the following to search by e-mail address:

   ```
   (&(|(ANR=$search$)(mail=$search$))(objectCategory=$userclass$))
   ```

> **TIP** Since this string uses the e-mail address of the user, and since an email address may not be unique in some systems, this is not the preferred option.

d. Click **OK**.

e. Open a command window, and reset IIS using the following command:

```
iisreset
```

For LDAP

a. Click the **Search Resolution** tab.

b. From **Available Attributes**, add both the following: `ANR`, and `userPrincipalName`.

c. Click **Add**.

d. Click **OK** to save.

e. Open a command window, and reset IIS using the following command:

```
iisreset
```

6. Log in to Aperture, and find an identity field, and verify that you can find one (and only one) user, searching with sample data that will be put in the `Name ID` of the SAML assertions.

   For example, if you're using UPN with Active Directory, log in as an AD user, and in a contact field search for a known email address in your organization (e.g. jane.doe@venafi.com) to make sure that one, and only one result is returned.

Now that you have configured the user lookup search expression, you're ready to move on to retrieving your Service Provider Metadata XML file.

Phase 1.4: retrieve Venafi Platform service Provider Metadata XML

In SAML authentication, the service provider (in this case Venafi Platform) publishes an XML metadata file, which is used for making the connection between the service provider and the identity provider. You need to export that file from Venafi Configuration Console using the following procedure.

To retrieve the service provider metadata XML file

1. Use Remote Desktop to connect to your Venafi server, and open Venafi Configuration Console.
2. Click the **Authentication** node.
3. Click the **SAML** component.
4. In the **Actions** panel, click **Properties**.
5. [Conditional] If requested, enter a master administrator username and password for Venafi Platform.
6. Select your **IdP Vendor** from the drop-down list.

   The settings window will populate based on your selection with the specific fields and terms for your identity provider.

   If you are using a non-tested IdP vendor, select **Other**, then enter the IdP name. This name will be used to identify the SAML configuration and for placing the certificate in the policy tree.
7. [Optional] Configure the **Default Return URL**. This is the default URL users will be taken to upon successful login through the SAML provider. Most organizations use `aperture`, as that is the most common starting place for users of the platform.
8. [Optional] Configure the **Log out URL**. If supported by your IdP, this is the URL that will trigger a log out of a session. As far as we know, Azure is the only tested IdP that supports a log-out URL.

   If your IdP does not support a Log out URL, and nothing is entered in this field, then Venafi Platform will not have a log-out option in the menu. After configuring this setting you need to restart IIS before you will see the change in the menu.
9. In the **Export and import SAML metadata** section, click **Export service provider file** and save the file to a location you'll be able to access during Phase 2.
   - Most identity providers can import the SP metadata XML file directly.
   - If your identity provider (including Okta) cannot import the SP metadata XML file, refer to the **Service provider details** for the URLs you will need when configuring your identity provider.

What's next?

When you've completed all four steps in phase one, you're ready to move on to phase two where you will configure your IDP.

While you *should* be able to connect Venafi Platform with any IDP that supports the SAML 2.0 standard, Venafi has tested and is providing guidance on using the following identity providers:

- "How to configure ADFS for SSO" on page 819
- "How to configure Azure for SSO" on page 822
- "How to configure Okta for SSO" on page 824
- "How to configure PingFederate for SSO" on page 826
- "How to configure PingOne for Enterprise for SSO" on page 831

NOTE Venafi Platform 25.1 only supports a single identity provider connection at a time. Multiple IDP connections may be considered for a future release.

How to configure ADFS for SSO

This topic details how to configure Microsoft Active Directory Federated Services (ADFS) for single sign-on (SSO).

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

ADFS is a common identity provider due to the integration with many organizations' existing identity infrastructure, while supporting SSO to cloud and other SaaS resources, even though ADFS typically sits behind the corporate firewall.

NOTE These setup instructions were written based on Windows Server 2016. If your Windows server is different, there may be minor adjustments you need to make.

You must have an existing functional ADFS deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to ADFS. The application is referred to in ADFS as a "Relaying Party Trust."

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via ADFS. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start

with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure ADFS for single sign-on

1. Log in to your ADFS Windows server and launch **AD FS Management** console.
2. In the Action Panel, click **Add Relying Party Trust**.
3. Click **Claims aware**, then click **Start**.
4. Select **Import data about the relying party from a file**.
5. Click **Browse**, and browse to the location where you saved the Service Provider Metadata XML file (done in "Prepare Venafi Platform for SAML SSO" on page 813).
6. Click **Next**.
7. Provide the Application (Relying Party Trust) name, then click **Next**.

   For example, you could enter something like: `Venafi Platform Production`.

   TIP If needed, you may want to differentiate between production, stage, and test environments.
8. Select who within you organization will be able to authenticate to Venafi Platform via ADFS, based on your access control policy and your discussions with your identity team and your machine identity management (or PKI) team, then click **Next**.
9. [Optional] Review, if desired, the data on the tabs on the **Ready to Add Trust** screen. These values were either set by you using the wizard, or were configured automatically from the Service Provider Metadata XML file you imported.
10. Click **Next**.
11. Leave **Configure claims insurance policy for this application** checked, then click **Close**.
12. In the **Edit Claim Insurance Policy** window you configure how ADFS identifies a user within the SAML assertion, and should match exactly the User Search Expression you used for Venafi Platform in "Phase 1.3: Configure SAML user search expression" on page 815.

    For example, if your search expression is `(&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))` then you are expecting a UPN to be specified in the SAML assertion created by ADFS.

If your search expression is `(&(|(ANR=$search$)(mail=$search$))(objectCategory=$userclass$))` then you are expecting an email address to be specified in the SAML assertion.

> **TIP** Active Directory does not enforce uniqueness of the email field, so be careful to choose attributes that are guaranteed to uniquely identify a user.

13. Click **Add Rule...**
14. Click Send **LDAP Attributes as Claims**, then click **Next**.
15. On the **Configure Claim Rule tab**, do the following:
    a. Give the rule a descriptive name.
    b. For the **Attribute Store**, select **Active Directory**.
    c. For **LDAP Attribute**, select **User-Principal-Name** (or whatever selection best matches your user search expression.)
    d. For **Outgoing Claim Type**, select **Name ID**.
    e. Click **Finish**.
16. Click your rule in the list, then click **OK**.
17. Open a PowerShell prompt (run as Administrator) on the ADFS server.
18. Enter the following command, replacing '<Name goes here>' with the name you gave your application earlier in the process:

```
Get-AdfsRelyingPartyTrust -Name '<Name goes here>' |Set-AdfsRelyingPartyTrust -SamlResponseSign MessageAndAssertion
```

    For example, if you used the name from our example, you would use the following PowerShell command:

```
Get-AdfsRelyingPartyTrust -Name 'Venafi Platform Production' |Set-AdfsRelyingPartyTrust -SamlResponseSign MessageAndAssertion
```

    This command sets an option that is not exposed in the ADFS UI to sign all SAML responses, which is a requirement of Venafi Platform.

19. From your ADFS server, open a web browser and visit:

https://localhost/federationmetadata/2007-06/federationmetadata.xml

We refer to this file as the *IDP Metadata XML file* in our documentation.

20. Download the federationmetadata.xml file to your Venafi Platform server as an XML file.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure Azure for SSO

This topic details how to configure Microsoft Azure for single sign-on (SSO). Azure is a cloud computing service used for building, testing, deploying, and managing applications through Microsoft-managed data centers.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional Azure deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to Azure.

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Azure. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure Azure for single sign-on

1. Log in to the Azure portal and go to **Enterprise Applications**.
2. Click **+ New application**.
3. Switch to the **old app gallery experience**.

4. Click **Non-gallery application**.
5. Enter a name for the Venafi Platform cluster you are integrating with, then click **Add**.

   This process may take a minute or more without a visual sign of progress, so be patient.
6. From the new application Overview page browse to **Manage** > **Users and Groups**, and click **+ Add user**.
7. In **Add Assignment**, click the **Users and Groups** bar to pull out a Users and Group list.
8. Enter the search pattern for the new group or user, select the new user from the results, and click **Select**.

   You'll be taken back to **Add Assignment**, where you will see a count of users selected.
9. Click **Assign** to complete the assignment
10. Click **Manage** > **Single sign-on** and select **SAML** as the single sign-on method.

    You'll see the **SAML-based Sign-on** page.
11. Click **Upload metadata file**.

    For the next step, you'll need the Service Provider Metadata XML file.
12. Browse to the Service Provider Metadata XML file you exported from Venafi Platform and click **Add**.

    You will see the contents of the XML file in the **Basic SAML Configuration** panel.
13. Click **Save**.
14. Close the panel and click **No, I'll test it later**.
15. In **User Attributes & Claims**, click **Edit**.
16. In **SAML Signing Certificate > Signing Option** select **Sign SAML response**, and click **Save**.
17. Close the panel and click **No, I'll test it later**.
18. In **SAML Signing Certificate** > **Federation Metadata XML**, click **Download**.

    The IDP Metadata XML file will be downloaded. Save it to a place where you will be able to find it easily.
19. In **Set up <APPLICATION NAME>** copy the **Logout URL** and paste it to a blank text file on the Venafi server.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure Okta for SSO

This topic details how to configure Okta for single sign-on (SSO). Okta is a common identity provider with wide application support.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional Okta deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to Okta. Consult the Okta documentation if you need to configure Okta to obtain data from your identity store.

Before you begin, you will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Okta. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure Okta for single sign-on

1. Log in to the Okta Classic UI.
2. From the menu, click **Applications** > **Applications**.
3. Click **Add Application**.
4. Click **Create New App**.

   You should see the **Create a New Application Integration** dialog box.
5. For **Platform**, select **Web**.

6. For **Sign on method**, select **SAML 2.0**.
7. Click **Create**.

   You should see the **Create SAML Integration** page, opened to step 1, **General Settings**.
8. Enter a unique name for the Venafi Platform cluster you are integrating with.

   The name must be unique in your Okta application list.
9. [Optional] Add a logo if desired, then click **Next** (leaving the boxes unchecked).

   You should see step 2, **Configure SAML**.

   Okta does *not* allow you to import the SP Metadata XML file, so for the next step, you will need to copy information from the **SAML Properties** window in Venafi Configuration Console.
10. In General settings:
    a. In **Single sign on URL**, paste the corresponding URL from the **Service provider details** section of the **SAML Properties** window in Venafi Configuration Console.

       For example: `https://test.venafi.com/aperture/api/saml/acs`
    b. Select the box for **Use this for Recipient URL and Destination URL**.
    c. Leave the box *unselected* for **Allow this app to request other SSO URLs**.
    d. In **Audience URI (SP Entity ID)**, paste the corresponding URL from the **Service provider details** section of the **SAML Properties** window in Venafi Configuration Console.

       For example: `https://test.venafi.com/aperture/api/saml/acs`
    e. Leave **Default RelayState** empty.
    f. For **Name ID format**, select **EmailAddress**.
    g. For **Application username**, select **Email**.
11. Click **Show Advanced Settings**, and complete the following fields:

Field	Value
Response	Signed
Assertion Signature	Unsigned

Field	Value
Signature Algorithm	RSA-SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	*Leave unselected*
Authentication Context Class:	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	*Leave blank*

12. Leaving all the rest of the attributes in their default state, scroll to the bottom of the form and click **Next**.

    You will be taken to step 3: **Feedback**.

13. Select **I'm an Okta customer adding an internal app**.

14. Click **Finish**.

    The application integration will be created, and you'll be taken to the application details page.

15. On the **Sign On** tab, under **Settings** > **Sign On Methods**, click **Identity Provider metadata**.

16. Download the IdP Metadata XML file on the Venafi Platform host.

    For example: `Okta-IdP-metadata.xml` (the file name is irrelevant).

    > **TIP** Make sure your text editor does not add any non-text characters to the file.

17. On the **Assignments** tab, click **Assign** > **Assign to people**.

18. For each user you want to be able to access Venafi Platform via SAML, click the **Assign** button next to their name, then click the **Save and Go Back** button.

19. Repeat the last step for each user, then click **Done**.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure PingFederate for SSO

This topic details how to configure PingFederate for single sign-on (SSO).

> **IMPORTANT** Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

PingFederate is an on-premise single sign-on (SSO) identity provider and directory service.

> **NOTE** These instructions were written based on PingFederate 10.2 on Windows Server 2016. If your server or software version is different, you will need to make necessary adjustments.

You must have an existing functional PingFederate deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform).

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Ping Federate. You'll need that information near the end of the procedure below.

> **IMPORTANT** While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure PingFederate for single sign-on

1. Log in to PingFederate on-premise, and open **Applications**.
2. From the side menu, click **Integration** > **SP Connections**.
3. Click **Create Connection**.

   PingFederate does not support the Service Provider Metadata XML file, which is why you can't click *Import Connection*.
4. In the SP Connections section:
   a. In the Connection Template tab

Field	Value
Template	Do not use a template for this connection

   b. In the Connection Type tab

Field	Value
Browser SSO Profiles	*Checked*
Protocol	SAML 2.0
WS-Trusts STS	*Unchecked*
Outbound Provisioning	*Unchecked*

Click **Next**.

c. In the Connection Options tab

Field	Value
Browser SSO	*Checked*
Attribute Query	*Unchecked*

Click **Next**.

d. In the Import Metadata tab

Field	Value
Metadata	File (radio button)

Then click **Choose File**, and select the Service Provider Metadata XML file you saved from Venafi Platform, then click **Next**.

e. In the Metadata Summary tab

Field	Value
Entity ID	*This field will contain the FQDN obtained from the XML file.*

Click **Next**.

f. In the General Info tab

Field	Value
Partner's Entity ID	*This field will contain the EntityID from the XML file.*
Connection	*This field will contain the Entity ID from the XML file. You can*

Field	Value
Name	*customize this, if you prefer.*
Base URL	*This field will contain the URL from the XML file.*

Click **Next**.

g. In the Browser SSO tab, click **Configure Browser SSO**.

- In the SAML Profiles sub-tab,
  - *Check* - **IDP-INITIATED SSO** (only works if Venafi Platform is reachable by IP address or FQDN)
  - *Check* - **SP-INITIATED SSO**.
  - *Unchecked* - **IDP-INITIATED SLO**.
  - *Unchecked* - **SP-INITIATED SLO**.
- In the Assertion Lifetime sub-tab, leave default settings.
- In the Assertion Creation sub-tab, click **Configure Assertion Creation**.
  - On Identity Mapping, select **STANDARD**.
  - On Attribute Contract select the following from the **SAML_Subject** dropdown: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - On Authentication Source Mapping, click **Map New Adapter Instance**.
    - For Adapter Instance, select **FederateUsers**.
    - For Mapping Method, select **Use only the Adapter Contract values in the SAML assertion**.
    - For Attribute Contract Fulfillment:

Attribute	Source	Value
SAML_SUBJECT	Adapter	username

    - For Issuance Criteria, leave empty.

- For Summary, review, then click **Done**.

  You'll be taken back to the Authentication Source Mapping page. Click **Next**.

- On Summary, review, then click **Done**.

  You'll be taken back to the Assertion Creation sub-tab. Click **Next**.

- In the Protocol Settings sub-tab, click **Configure Protocol Settings**.
  - On Assertion Customer Service URL, accept the default settings.
  - On Allowable SAML Bindings:

Field	Setting
Artifact	*Unchecked*
Post	*Checked*
Redirect	*Checked*
SOAP	*Unchecked*

  - On Signature Policy:

Field	Setting
Require Authn Requests...	*Unchecked*
Always sign assertion	*Checked*
Sign Response as required	*Checked*

  - On Encryption Policy, accept the default settings (none).
  - On Protocol Settings Summary, review, then click **Done**.

    You'll be taken back to the Protocol Settings page. Click **Next**.

- In the Summary sub-tab, review, then click **Done**.

  You'll be taken back to the Browser SSO tab. Click **Next**.

h. In the Credentials tab, click **Configure Credentials**.

- In the Digital Security Settings sub-tab:

Field	Value
Signing Certificate	*Select any; If none exist, click Manage Certificates to either create one or import one for use.*
Signing Algorithm	RSA SHA256

- In the Summary sub-tab, review, then click **Done**.

  You'll be taken back to the Credentials tab. Click **Next**.

i. In the Activation and Summary tab, review your selections, then click **Save**.

   You'll be taken back to the SP Connections section, where you can see the newly-created connection.

5. In the SP Connections section, locate your newly-created connection, then click **Select Action** > **Export Metadata**.
6. On the Metadata Signing sub-tab, select any signing certificate, and select the **RSA SHA256** signing algorithm, then click **Next**.
7. On the Export & Sumary sub-tab, click **Export**. We refer to this file as the *IDP Metadata XML file* in our documentation.

   You'll need to save this to your Venafi Platform server, in a place you can find it later.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure PingOne for Enterprise for SSO

This topic details how to configure PingOne for Enterprise single sign-on (SSO). PingOne for Enterprise is a cloud-based authentication provider.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional PingOne for Enterprise deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to PingOne. Consult the PingOne for Enterprise documentation if you need to configure PingOne to obtain data from your identity store.

Before you begin, you will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via PingOne for Enterprise. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure PingOne for Enterprise single sign-on

1. Log in to PingOne for Enterprise, and click **Applications**.
2. Navigate to **Add Application** > **New SAML Application**.
3. Give the application a descriptive name for your Venafi cluster, and provide a description and choose a category.
4. Click **Continue to Next Step**.
5. Next to SAML Metadata, click **Download**. We refer to this file as the *IDP Metadata XML file* in our documentation..

   Save this file to your Venafi Platform server in a place you can find it later.
6. Ensure the protocol version is **SAML v 2.0**.
7. Under Upload Metadata, click **Select File**, then browse to the Venafi Service Provider Metadata XML file you exported from Venafi Platform, and select it.
8. The following fields are described below:
   - The **Assertion Customer Service (ACS)** field will be automatically filled out from the uploaded Service Provider Metadata XML file.
   - The **Entity ID** will be automatically filled out from the uploaded Service Provider Metadata XML file. This is a unique string PingOne uses to identify the application when communicating with it.

- For **Application URL**, you can leave blank.

  This feature, if used, provides the starting URL for a user, if you don't want them being taken directly to the Aperture dashboard. For example, you could specify the SSH Protect dashboard, or the Certificate Inventory URL. This URL will be used when a user clicks on the Venafi application on their PingOne dashboard. This field is not honored if authentication was started by Venafi Platform. If you use this field, use the FQDN to the page.

- **Single Logout Endpoint, Response Endpoint, Binding Type**. These settings are not supported in this version of Venafi Platform, so leave blank.

- **Primary/Secondary Verification Certificate**. Since version 25.1 doesn't support signing authentication requests, leave blank.

- **Encrypt Assertion**. Since version 25.1 doesn't support encrypted SAML responses, leave blank.

9. Change the Signing option to **Sign Response**.
10. Leave the Signing Algorithm to the default, which is **RSA SHA256**.
11. If you want to force re-authentication for users, even if they already have an active PingOne session, select **Force Re-Authentication**.
12. If needed, modify the subject of the SAML assertion.

    By default, PingOne sends the username as the NameID within the subject of the SAML assertion. If you need to have something different sent instead (like email address), you need to define appropriate attribute mapping on this screen.

    More information can be found in PingOne's documentation.
13. In Group Access, click **Add** next to groups that should have access to Venafi Platform.

    If you want all users to have access, click **Add** next to **Users@directory**.
14. Review your settings, then click **Finish**.

> **IMPORTANT** When you test PingOne, if you get an error on a login attempt that says "SAML authentication failed" with an InvalidSignatureException, try disabling assertion signing in step 9, above. This is due to a problem in .NET.
>
> If disabling assertion signing doesn't work, please contact Venafi Support.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML

After you configure your identity provider (IDP), you are ready to go back into the Venafi Configuration Console to finalize the configuration. During this process, you will upload the IDP Metadata XML. This file contains configuration information that Venafi Platform needs to properly configure your SAML connection to the IDP.

This topic is part of Phase Three (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

To import IDP Metadata XML into Venafi Platform

1. Use Remote Desktop to connect to your Venafi server, and open Venafi Configuration Console.
2. Click the **Authentication** node.
3. Click the **SAML** component.
4. In the **Actions** panel, click **Properties**.
5. [Conditional] If requested, enter a master administrator username and password for Venafi Platform.
6. [Conditional] If not previously selected, choose your **IdP Vendor** from the drop-down list.
7. In the **Export and import SAML metadata** section, click **Import identity provider file**
8. Browse to the location of the IdP SAML file on your system, click the file, then click **Open**.
9. If your IDP support it, you can provide a **Logout URL**.

   If a value is not provided, you won't see a Logout link in the menu. Of the IDPs tested by Venafi, only Azure supports logging out by URL.

   If there is no Logout link, users will close their browser to terminate a session.
10. Click **Save**.

    The **SAML Properties** window closes.
11. In the **Actions** panel, click **Enable**.

Managing the SAML certificate in TLS Protect

The IdP Metadata XML file contains a TLS certificate that is automatically enrolled in TLS Protect at the *monitoring* level. This means you can see the SAML certificate in the policy tree, and you can see (and monitor) its expiration like you do for your other certificates.

The enrollment level is monitoring because TLS Protect can't renew and provision a new certificate. To renew this certificate, you must export a new IdP Metadata XML file from your identity provider and upload it into the Venafi Configuration Console. When you import a replacement IdP Metadata XML file, the old certificate is placed in the history of the new certificate.

The location of the certificate in the policy tree is shown in the **SAML Properties** panel after you upload your IdP Metadata XML.

What's Next

If everything is configured correctly, SAML authentication should now work. We recommend opening another browser or incognito window and open Aperture. You should be redirected to your IDP login page. If you enter valid credentials, you should be taken to Aperture.

If you are having troubles, check out some "SAML troubleshooting tips" on page 835.

SAML troubleshooting tips

If your SAML SSO integration is not working, here are some things you can try.

Check the Venafi Platform logs. Venafi Platform has very detailed logging for SAML Authentication when an error is encountered. Start with the Venafi Configuration Console Log Viewer. For example:

1. In Venafi Configuration Console, Expand the **Venafi Event Viewer** node.
2. Right-click on **Custom Views** and click **Create Custom View**.
3. In the **Logged** field, choose **Last Hour**.
4. For **Event Sources**, choose the parent **SAML Group** node, then click **OK**.
5. Give the custom view a **Name**, like `SAML Last Hour` and place it in the **Custom Views** container.

You now have an easy to use log view for troubleshooting SAML issues.

Enable Debug Logging for your UI Server. In Policy Tree on the Platform tree, you can select your servers that have "Web Console" enabled and activate debug logging temporarily. Additional logs will be stored, like your SAML Assertion, which is helpful for understanding what was sent and received between Venafi Platform and the SAML Identity Provider (IDP).

Make sure your FQDNs are configured. By default, email notifications and your SAML configuration use your windows machine `hostname` to build URLs. This is typically *not* the URLs you want to use in either lab or production environments. Instead, we recommend putting in a fully qualified domain name (FQDN) that matches the trusted Venafi Operational Certificate you have installed on Venafi Platform. Once this is

set, you may need to re-export your Service Provider Metadata XML file from the Authentication node of the Venafi Configuration Console, and use the updated file to re-configure your settings with the Identity Provider.

Type the correct domain name in your browser. If your Venafi Platform is configured to use `platform.example.com` don't use the machine's IP address or `localhost` when accessing your SAML-enabled server. An error can occur, because Venafi Platform will redirect you to your identity provider. Your IDP will generate a signed SAML response using the domain name you configured (for example, `platform.venafi.com`) If the domain name that your IDP uses is not the same as the one you entered in your browser, Venafi Platform will reject the SAML response from your IDP for security reasons.

Check the value in the `NameID` within the subject section of the SAML assertion of your SAML Response. A SAML Response can be several hundred lines long, but in every response you should see a basic structure to include a `NameID` that tells your server "this is the user who I am authenticating."

```
<samlp:Response>
    <saml:Assertion>
        <saml:Subject>
            <saml:NameID>aaron.hixson@venqa.venafi.com</saml:NameID>
        </saml:Subject>
    </saml:Assertion>
</samlp:Response>
```

You should know what type of identification you are using to identifying users. We recommend using a `User Principle Name` (UPN) because it always uniquely identifies a user within a given directory. However, there are other alternatives.

When looking at the SAML response, you're looking for two things:

1. Check that the SAML Response `NameID` matches the user identifier you are expecting. If yes, go to the next step.
2. Turn off SAML on Venafi Platform and authenticate to Aperture as a user from that Identity Provider. For example, if your IDP uses Active Directory, try logging in to Aperture with a valid AD user and password. Once in Aperture, take the string from the `NameID` and try to search from the user. In our example, search for a `UPN` of `aaron.hixson@venqa.venafi.com`. If there are no results, then you probably have one of the following problems:
    - Your User Search Expression for your Identity Provider doesn't include the attribute for user class objects that this attribute is stored on.

For example, for UPN you didn't change your Active Directory user search expression to: `(&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))`

- If using Active Directory, you may have expected the attribute to be included in your directory's "Ambiguous Name Resolution" (ANR). By default, Venafi Platform's Active Directory driver searches for users using ANR. While Microsoft documents what the default attributes are for ANR, your Active Directory Administration team may have removed or added attributes that are different from Microsoft's default settings.
- Your identity directory does not have the values you think it does. Let's say for example your Identity Provider has `employee ID`, and you thought Active Directory or LDAP also had an `employee ID`, if that is not the case, you should switch to a different unique attribute like Universal Principal Name (UPN). As mentioned before, a good test is to log into Aperture and try to search for the user using the desired attribute, if nothing shows up, then that problem needs to be resolved first.

Ensure you are using a unique identifier. If you are trying to use something like `email`, `username`, or `SAMAccountName` as the value in your `NameID`, it's possible that these values are returning multiple results when Venafi Platform searches your IDP's directory. When an Identity search returns multiple entries, the SAML Assertion is rejected because the lookup for a user is ambiguous. A match will only be made if there is one–and only one–user that matches the `NameID` of the SAML Assertion subject.

When looking at the log, if you see a log event similar to the following, this is likely your problem.

> Ambiguous identity lookup by name id (admin). Found identity entries: (local:{c6b377a2-8e8a-4cd8-cee9-9690f0d988a3}, LDAP+odsee:6c512d81-48f711a2-80d19f9-b115de56).

Your IDP is not signing the SAML Response. Venafi Platform requires SAML Responses to be signed, but with the exception of Okta, all of the IDPs that Venafi supports, by default, only sign the *assertion* within the response. When setting up your IDP to work with Venafi Platform, make sure Venafi Platform's application profile is configured to sign the *response*.

Time Sync Problem. Venafi Platform requires that the SAML Assertion include the `NotOnOrAfter` parameter within the `SubjectConfirmationData` of the assertion. This is to prevent the possibility of misuse of the signed XML document. Venafi Platform allows for a clock skew of 180 seconds (3 minutes). Check to make sure that the system time of your IDP and the system time of your Venafi servers are all accurate.

Other tips and information

- We suggest you try the Firefox SAML Tracer Extension, a valuable tool that picks through the network traffic and highlights the SAML XML documents that Venafi Platform and your SAML IDP are sending back and forth through your browser. While you can get this information if Venafi Platform is in Debug Mode, and you look through the logs, this extension provides real-time information, which is faster and simpler than using the system logs. In addition, in some customer environments, Debug Mode isn't allowed or is not a practical solution.

  > **TIP** Make sure you have the extension open *before* you visit your IDP or Venafi Platform's web console. The SAML Tracer Extension only captures traffic when the extension window is open.

- If you're looking for the Logout button in Venafi Platform's navigation, you should know that the Logout button isn't visible when SAML single sign-on is enabled. In Venafi Platform 25.1, we don't support SAML Single Log Out (SLO). What we do support is a **Logout URL**. If your IDP supports ending the session by simply visiting a URL, you can place that URL in the **Logout URL** field. After you set this, restart IIS and you should see the Logout link in the User menu of the Venafi Platform web console.

  As far as we know, Azure may be the only supported IDP that permits logging out by just visiting a URL. Azure users can use the following **Logout URL**:

  ```
  https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
  ```

Venafi Recycle Bin

Sometimes users delete items that they shouldn't, or items they later regret deleting. The recycle bin allows a system administrator with the Master Admin role and/or the Recycle Bin Administrator role to undo the deletion of certain objects using Venafi Configuration Console or the Venafi MMC snap-in.

For more information about the Recycle Bin Administrator role's capabilities and limitations, see "Understanding system roles" on page 706.

The recycle bin allows you to safely automatically cleanup old archived machine identities, knowing that you can quickly restore them if needed (within a specified time period).

The recycle bin allows you meet your specific business requirements, such as the following:

- Automatically remove certificate data (or historical certificate data) from secret store that expired *X* years ago.
- Exclude certain information from being deleted.
- Review logs for deleted identities for auditing purposes.
- Restore a deleted machine identity when a server owner calls in a panic saying they deleted it by accident.

Please note that you can use TppTool to perform many recycle bin actions from the command line and script files. See" Using TppTool from the command line and script files" on page 519.

Scope

IMPORTANT Not everything that is deleted in Venafi Platform can be restored from the recycle bin. For example, while certificates, policies, and credentials are generally recoverable, some objects cannot be restored. **This feature is not a global "undo."** It does, however, allow you to restore the most critical objects in the case of accidental deletion by the clean up process, or by a user.

The following objects ARE generally recoverable (see exceptions, below).

- Policy settings, certificates, and provision settings such as credentials, and Application objects.
- Logging channels and notifications.
- SecretStore Vault owner and entry information.
- Devices.

  WARNING! Any SSH keys that are associated with the device are not currently recoverable. Deletion of a device removes all SSH keys from SSH Protect's inventory, but this does not deprovision the keys from the device. So the keys will still be able to connect to that device. For additional information see "How SSH Protect uses the recycle bin" on page 151.

- SSH certificate issuance templates.
- SSH certificate issuance flows.
- Adaptable actions for SSH certificate issuance flows.
- SSH CA keypairs.

The following items are NOT recoverable:

- Agent/Client Registrations within the Client Subsystem.
- API Integration registrations within the OAuth Subsystem.
- Preference changes or deletions.
- Attributes on specific objects (Recycle Bin covers deletion of the object itself, not the deletion or changing of configuration options on the object).
- Permission assignment, Workflow ticket, or Flow ticket deletions.
- Device information. Any SSH Keysets, key instances, and trust information that is not stored in the Recycle Bin is deleted immediately.
- SSH keys. SSH Protect documentation provides details on how the recycle bin treats SSH assets.

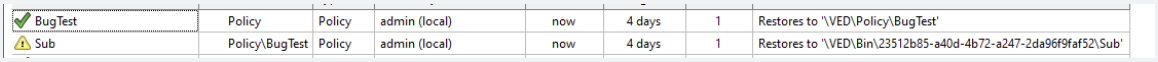
> **NOTE** Deletion of SSH keys from the inventory does two things: First it removes the keyset from SSH Protect's inventory, and second it deprovisions the keys on the connected devices. This means the public key is removed from the `authorized_keys` file on all connected devices. The keyset will no longer be able to connect to that device.

Restoration Availability

Each entry in the recycle bin has an icon that tells you the availability of an entry to be restored. The last column of the table where the item will be restored to.

Icon	Description	Details
	Green check mark indicates the item can be restored to its original location	To restore this item, click the **Restore** action.
	Yellow warning icon indicates the item's parent is also deleted so it can't be restored.	To restore this item, restore it to its parent, then restore its parent.
	Red circle with line indicates the item cannot be restored as is.	For details on why this can't be restored, click **Properties**.

EXAMPLE The following graphic shows two items in the recycle bin. `BugTest` is a parent item that contained `Sub`, but they were deleted in different actions. `Sub` item has a yellow warning icon, indicating that it can't be restored directly to is original location. (Note how in the last column it shows that the item will restore to the `\Bin\`).



BugTest	Policy	Policy	admin (local)	now	4 days	1	Restores to '\VED\Policy\BugTest'
Sub	Policy\BugTest	Policy	admin (local)	now	4 days	1	Restores to '\VED\Bin\23512b85-a40d-4b72-a247-2da96f9faf52\Sub'

If you want to restore Sub you have two options:

- Click **Restore** for the `Sub` entry. It will be restored to the `BugTest` item still in the recycle bin (note you can see this in the last column)
- Click **Restore** for the `BugTest` entry. It will be restored to its original location in `\Policy\`. The `Sub` item will now have a green check mark because it can be restored to its parent in `\Policy\BugTest`.

For details on any entry, click the **Properties** action which will provide detailed information about the entry's restore state. There you can see extensive information about the entry including:

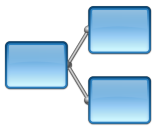
- The entry's original location.
- Restoration information, including how and where an item will be restored.
- A detailed explanation of why a given item cannot be restored.
- Information about who deleted the item and when.
- Information about when the item will automatically be purged if no action is taken.

If you click **Retrieve Details** before you click **Properties**, you can see even more information including:

- Number of associated vault (Secret Store) entries
- The types and counts of items of those types in Secret Store.

Other icons

When you **Retrieve details** of an entry, the associations are shown in an expandable sub-list. These items have one of two icons, as outlined in the following table.

Icon	Description
	The branch icon indicates the linked item is *not* stored in the Secret Store vault.
	The key icon indicates the linked item *is* stored in the Secret Store vault.

Restoration exceptions and potential resolutions

There are a number of reasons why you might not be able to restore an item in the recycle bin. Here are some of the more common scenarios:

Case	Resolution Options
A child item is deleted in one step. Later the child's parent is deleted in a different step.	1. Click "Restore" on the child item and the association with the parent is restored, however, they are both still in the recycle bin. If you restore the parent item at this point, both the parent and the associated child item will be restored. 2. Restore the parent item. The child item can then be restored to its original parent. (In this case, not that after the parent item is restored, the child item's icon changes to a green check mark.) 3. Purge the parent item so it is no longer in the recycle bin. Then create a new parent item in the same location with the same name. If you click Restore on the child item at this point, the child will be restored to the new parent you created.
A child item gets deleted. Later the child's parent is renamed.	If you restore the child item, Venafi Platform will attempt to restore the item to the renamed parent item, if the renamed parent still exists.

Accessing the recycle bin

The recycle bin interface can be accessed in three ways:

- By connecting to the Venafi Platform server and opening Venafi Configuration Console (VCC). The Recycle Bin node is in the left panel.

- By adding the MMC snap-in, and assigning both the application entitlement, as well as assigning the user master admin permissions.
- By connecting to the Venafi Platform server and using the command line. For more information, see .

Recycle Bin event logging

Detailed information about all recycle bin events can be seen in the Venafi Event Viewer. This tool is available in Venafi Configuration Console, or as an MMC snap-in. For details on the Event Viewer, see "Venafi Event Viewer overview" on page 375.

In the Venafi Event Viewer you can use the filter function to only see Recycle Bin events, or even specific types of Recycle Bin events. You can save these as a custom view to refer back to them easily. To learn how to create custom views, see "Custom Views" on page 376

Related API documentation

Systems accessing Venafi Platform via the API can interact with items in the recycle bin. For more information, see RecycleBin API.

What's next?

If you are looking for general information about the recycle bin interface, see "Recycle Bin's interface" below.

If you are trying to restore an item that was deleted, see "Recycle Bin's actions panel" on page 145

If you are wanting to learn more about a specific recycle bin item, see "Recycle Bin's details panel" on page 150.

Recycle Bin's interface

The recycle bin is a node in the Venafi Configuration Console and the MMC snap in. Only users with the master admin role can access it[1]. If you are trying to restore an item you deleted, and you aren't a master administrator, please reach out to your Venafi administrator for assistance.

When you open the recycle bin node you see rows for "entries" which are groups of items recently deleted. These may have been deleted by a user, or they may have been deleted by a process.

---

[1]Users with the MMC snap-in will need the appropriate application grant for the recycle bin. If they have the grant, but are not master administrators, they will see the Recycle Bin node, but it will be empty.

By default, the recycle bin node retrieves and displays up to 2500 objects. In the upper-right corner of the center panel you can see how many items, in total, exist in the recycle bin. Displaying more can increase load time, but if you want to, you can increase the limit using the **Retrieve** drop-down.

Recycle Bin entries can contain multiple items. For example, if you delete one certificate object, you will get one entry (one row). However, this deletion may have included the active certificate, the related keys, as well as any historical certificates that were previously archived. To see what items are part of an entry, click on the entry, then click the **Retrieve details** action in the **Actions** panel. The list of items will be retrieved, and you can use the expand icon (in the **Container** column) to see all the items in the group.

Three types of entries can be seen in the recycle bin:

- **Configuration objects**: items, and collections of items, like policy folders. If the item has no children, then configuration objects only contain one item. However, if the configuration item has children (like a policy folder that contains other policy folders or machine identities), then these will be represented as different items within an entry. The child objects can be of any of the three object types.
- **Vault entries**: items (like machine identities, credentials, etc.) that were stored in Secret Store. These are single items that were removed from their owner.
- **Owner entries**: collections of Secret Store vault items that were all owned by a particular owner, and the ownership was deleted. For example, a private key and a certificate.

To see detailed information about an entry, click the entry, then click **Properties** in the **Actions** panel.

While the columns on the Recycle Bin node are self explanatory, please note the following:

- They time columns can toggle between relative times (2 hours ago; in 14 days) and absolute times (represented with the date of the event). The column title changes depending on the toggle state. The toggle icon is in the upper-right corner of the table. (Note that if you modify the purge settings in **Configuration**, this list automatically updates.)
- Like all tables in the management console, columns can be sorted, and rearranged with drag-and-drop. Right click on a column header for additional options.

The recycle bin will not automatically refresh to show new objects that are deleted while you have the node open, but you can click the **Refresh** action in the **Actions** panel.

> **NOTE** There is a configuration that exists on all WebAdmin policy objects called **Exclude from automatic deletion**. When this setting is enabled, these objects will be ignored by the automatic deletion features of the Recycle Bin.

Advanced Recycle Bin features

There are several advanced recycle bin features that are available using the recycle bin's command line tool on the Venafi Server. For example, you can force the deletion task to run immediately using the command line tool.

For details about how to use the command line Recycle Bin utility, see .

What's next?

If you want to restore an item from the recycle bin, see "Recycle Bin's details panel" on page 150

If you want to learn more about the actions and configuration options, see "Recycle Bin's actions panel" below

To understand the business case for recycle bin, see "Venafi Recycle Bin" on page 138.

Recycle Bin's actions panel

The Actions panel has the following options. When reviewing the following note the difference between *deletion tasks* and the *purging* of data. A deletion task can find old data in Secret Store and automatically move it to the recycle bin. Purging data is the process of permanently "emptying" the recycle bin.

- Configuration...

  Purge items deleted more than ... - Changes the settings for how the *purge* action works. You can determine the length of time items in the recycle bin can remain before they are purged.

  Limit purge process runtime... - You can limit the amount of time a purge process can run (to minimize impact on other resources).

  Engine to run... - You can select which Venafi Platform engine performs the purge tasks, which also allows you to minimize impact on other server processes.

  The default settings are to purge deleted items more than 14 days old, to limit process runtime to 3 hours, and to use any available engine. If you modify these settings, the entries list in the recycle bin immediately updates to show the new automatic purge date[1].

[1]For added clarification: the age of items is calculated when the Purge process runs. If you change your settings, they will apply immediately both to already deleted items as well as future items.

The purge process runs with other daily tasks that run on the server. By default, the server runs daily tasks at midnight. You can modify this in engine's settings on the engine settings.[1]

If there are more items to purge than the limit imposed by the above settings, the purge process will continue during the next task window. The process will continue until all items have been purged from the system.

As a system administrator you may want to routinely monitor the recycle bin's logs in the Venafi Event Viewer to ensure old data is being purged at an appropriate rate. If you aren't purging a sufficient number of items, you can increase the runtime.

If you have been using Venafi for a long time, or if you have a lot of old data in your system, this process may initially take several days (or even weeks) to complete. After the initial purge has completed, you should adjust your settings to ensure enough items can be purged each day.

The process was designed to minimize impact to system resources, but if you find that deletions aren't happening as quickly as you expected, or if you notice an impact on performance, you might try setting up a new engine specifically for deleting and purging.

- ### Deletion Tasks...

  To minimize storage space and to comply with industry or organizational policies, Venafi Platform can regularly clean up old data that may no longer be useful. We call this cleanup process "Deletion Tasks." The **Deletion Tasks...** action lets you customize your cleanup settings.

  To customize settings related to performance, you can adjust the following settings:

  - **Limit deletion process runtime.** Configure the length of time the recycle bin can spend working on an automatic deletion action. The default is 3 hours.
  - **Engine to run deletion process.** Specify which engine performs the deletion tasks.

    > **TIP** If you need improved performance, consider creating an engine specifically for deleting and purging.

  - **Delete a maximum...** Choose how many entries are deleted in a given task. The default is 1000 entries.

[1] If you want to change this setting, open **Policy Tree** and browse to the **Platforms** tree. Expand the **Platforms** tree and click on the engine. In the **Venafi Protection Platform** tab, open the **Settings** sub tab. The setting is called **Run daily tasks at**.

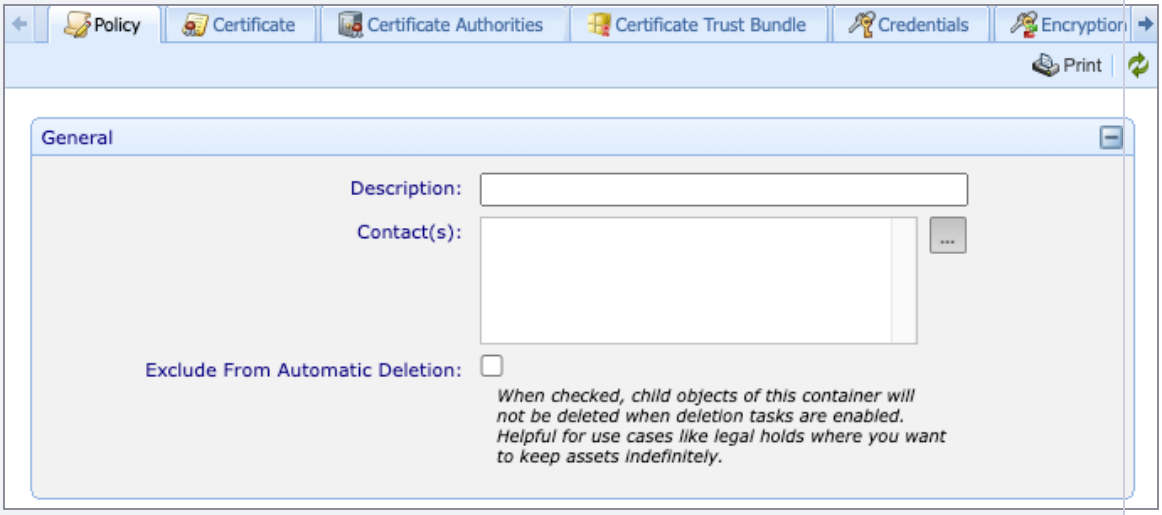
When the system reaches *either* the time limit *or* the number of entries limit, it pauses processing deletion tasks, and waits for the engine's next task window to continue. The process will continue until all items have been deleted and moved to the recycle bin.

As a system administrator, you may want to routinely monitor the recycle bin's logs in the Venafi Event Viewer to ensure old data is being moved to the recycle bin at an appropriate rate.

If you have been using Venafi for a long time, or if you have a lot of old data in your system, this process may initially take several days (or even weeks) to complete. After the initial deletion tasks have completed, you should adjust your settings to ensure enough items can be automatically deleted each day.

NOTE There is a configuration that exists on all WebAdmin policy objects called **Exclude from automatic deletion**. When this setting is enabled, these objects will be ignored by the automatic deletion features of the Recycle Bin. A use case for this feature is when there is a legal hold where you want to maintain assets indefinitely.

From the menu, click **Policy Tree**, then click on a policy object (not on a certificate object). Look at the **Settings** tab, **Policy** sub-tab. In the **General** section, you can click **Exclude From Automatic Deletion**.

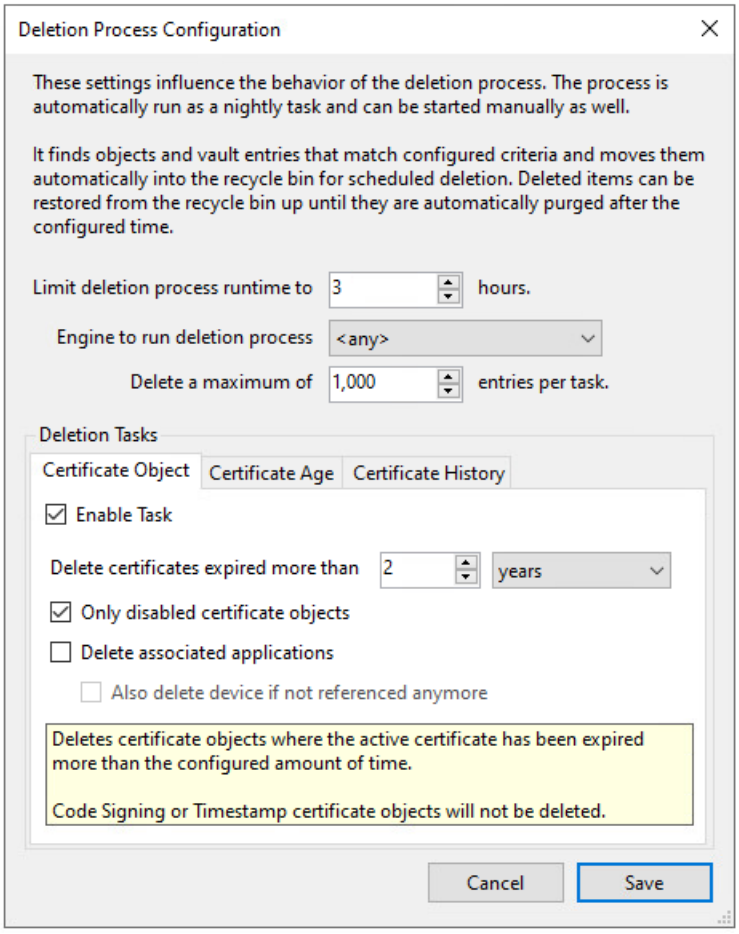


Determine which deletion tasks are run (Deletion Tasks tabs).

You can automatically clean up X.509 certificates (not SSH certificates or code signing certificates) based on the following system parameters. If you would like to have certificate objects cleaned up then please enable and configure the **Certificate Objects** deletion task.

The **Certificate Age** and **Certificate History** deletion tasks are configured to operate exclusively on archived certificates. This ensures that only those certificates specifically designated for deletion are processed.

Each type of deletion task has its own tab on the Delete Process Configuration screen.



- **Certificate Object**: Considers details about the certificate object's active certificate to determine if the certificate object should be deleted. The settings are:
  - **Enable** or disable this deletion task.
  - Specify the time period to use for deletion. Certificate objects that **expired** longer ago than the specified time would be considered for deletion, based on the other settings on this tab.

- Choose if you want to delete all certificates, including old active certificates, or if you only want to **delete *disabled* certificate objects**.
- Choose if you also want to **delete associated applications**.
- If you do delete the applications that used this certificate object, you can also delete any unreferenced **devices**. This can help maintain an accurate list of devices by helping prevent orphaned device objects.

◦ **Certificate age**: Deletes certificate data for *all* certificates[1] that are older than a specified number of years[2]. The settings are:

◦ Enable or disable this deletion task.

◦ Specify the time period to use for deletion. Certificates older than this age will be deleted and moved to the recycle bin.

◦ Specify whether *active* certificates can be deleted, or if only *archived* certificates (but not the most recent archived certificate) are deleted. When this option is selected, only archived certificate data (older than the most recent certificate) will be deleted.

◦ **Certificate history**: Determines the number of versions of a certificate are retained. This allows you to maintain, for example, the Secret Store data from the five most recent versions of a certificate, but if seven historical certificates are found, it will delete the Secret Store data of the oldest two, so five versions would remain in history. The settings are:

◦ Enable or disable this deletion task.

◦ Specify the number of versions of a certificate to retain.

■ **Purge all...** or **Purge all in background...**

Performs an immediate, irreversible purge of all items in the recycle bin. By default, a confirmation modal appears, which can be disabled.

[1]This is not just certificates in the Policy tree; it is all certificates that meet the criteria. For example, it also deletes data for a Discovery job's archived certificates, certificates in the roots tree, etc.
[2]The Certificate Object deletion task deletes the certificate objects themselves. The Certificate Age deletion task deletes *certificate data* associated with certificate objects, but does not delete the objects themselves.

The label depends on the amount of data in the recycle bin. If the amount of data to purge is small, you see **Purge all...** and the system purges the data while you wait. If the amount of data would take a longer time to purge, you see **Purge all in background...** which starts the purge as a background task so you can continue using the snap-in or console. If you click Refresh in the console, the refreshed contents will allow you to see how far the purge has progressed.

- **View**

  An MMC standard action that lets you customize the view of the overall console and which has not been modified by Venafi.

- **Refresh**

  Perform an immediate refresh of the contents of the recycle bin. As you take actions on the recycle bin, it automatically refreshes. This option allows you to refresh without taking any other action.

What's next

If you want to take action on a single recycle bin entry, see "Recycle Bin's details panel" below.

If you want to see the recycle bin events in the Events Viewer, see "Venafi Event Viewer overview" on page 375

For information about the recycle bin main panel interface, see "Recycle Bin's interface" on page 143.

Recycle Bin's details panel

You can view information about an individual entry or item in the recycle bin by clicking on the actions available for that item.

In Venafi Configuration Console, when you click on an entry or item in the recycle bin, you see options in the bottom part of the **Actions** panel in a section with the title of the entry or item you have selected.

If you have selected an entry, you have the following options:

- **Restore**. Restore all items in the entry to their previous locations.

  You cannot restore individual items in the entry. You must restore the entire entry.

- **Purge**. Immediately purge the selected entry from the recycle bin. It will then be irrecoverable.

- **Retrieve details**. If a entry has child items, click to retrieve the list of all child items. An expand icon will appear in the **Container** column. Click the icon to see all the individual child items.

These child items *only* have the **Properties** action, as they cannot be individually purged or restored.

- **Properties**. Display a modal window with detailed information about the entry or item.

  Properties provides a detail-rich description of the entry or item. You can see:

  - The entry's original location.
  - Restoration information, including how and where an item will be restored.
  - A detailed explanation of why a given item cannot be restored.
  - Information about who deleted the item and when.
  - The number of vault entries contained in the config entry, as well as a list of vault types, with a count of how many of each type are included.
  - Information about when the item will automatically be purged if no action is taken.

  If you click **Retrieve Details** before you click **Properties**, you can see even more information including (when applicable):

  - Number of associated vault (Secret Store) entries
  - The types and counts of items of those types in Secret Store.

What's next?

If you prefer to interact with the recycle bin via the command line, go to .

If you wanted to verify the restoration, go to the web interface where you can see the restore item in the expected location.

If you want to take actions on the entire contents of the recycle bin, see "Recycle Bin's actions panel" on page 145.

How SSH Protect uses the recycle bin

The recycle bin is a feature in Venafi Configuration Console that allows system administrators to restore some object types if they are deleted either by accident, or in the case of TLS certificates, if they are pruned during the automated cleanup process called Deletion Tasks.

If you are not a system administrator, and you want to recover a supported item that you deleted, please contact your Venafi administrator.

It is important to understand how the recycle bin works with SSH Protect assets, as some objects are recoverable and some are not.

SSH Protect items that can be recovered

The following items can generally be recovered by a system administrator from the recycle bin if their parent container was not deleted after the item:

- SSH certificate issuance templates
- SSH certificate issuance flows
- Adaptable actions for SSH certificate issuance flows
- SSH CA keypairs
- Device objects (but *not* their associated keys)

SSH Protect items that cannot be recovered

The following items are not recoverable:

- SSH keys.

  The deletion of SSH keys is permanent.

  When you delete a keyset in SSH Protect, the system deprovisions the keys from any associated devices. This means they public key is removed from the `authorized_keys` file on the devices. This keyset will no longer allow any client to connect to that device with that keyset.

- SSH Keys linked to devices.

  When you delete a device from SSH Protect, the system does not deprovision the keys associated with the device, but *those keys are removed* from the SSH Protect inventory.

If you need to restore a deleted key or device that can't be restored by the recycle bin, you will need to add new SSH keys and or devices to the same location on the device, or perform another discovery of the device.

What's Next?

To learn more about the recycle bin, see "Venafi Recycle Bin" on page 138.

To learn about TLS certificate deletion tasks, see "Recycle Bin's actions panel" on page 145

Access Management

The access management node in Venafi Configuration Console (and the matching MMC snap-in) allows you to configure and manage access to Trust Protection Platform by way of Venafi's public APIs.

Equivalent functionality can be accessed using the OAUTH endpoints in the public API. For detailed information, see Grant management endpoints.

The access management overview page gives you a brief overview of the access that has already been granted, as well as a list of current global access management settings.

There are several possible actions on the overview page. Your ability to see or use them will depend on the role assigned to your identity. For information about roles in access management, see "Using roles for access management in Venafi Configuration Console" on page 396. Possible actions include:

- Change Global Settings
- Revoke User Grants
- Delete Identity Rules

Change Global Settings

Depending on your role, you may have the ability to view or edit global settings.

Tab	Field	Description
General	Username + Password	The client passes a username and password to the VEDAuth server. This is the same username and password that could be used to log in to the web console. Learn more about username and password authentication.
General	Integrated (Windows) Authentication	The client passes Windows credentials to Venafi for access. Learn more about Windows authentication.

Tab	Field	Description
General	Json Web Token (JWT)	A token in JSON format that is used to communicate between a trusted identity provider and Venafi Platform. Learn more about JWT authentication.
Certificate	Enabled	The caller passes a client certificate to Venafi for access. Learn more about certificate authentication.
Certificate	User identity field	The field from the X.509 certificate used to match the certificate with an identity in the system. ■ You can specify an SID as the certificate field and specify a backup field if the SID is not found. ■ You can choose to always use a selected certificate field.
Certificate	Client certificate issuers	The CA(s) that are approved to issue client certificates for authentication. You can select one or more client certificate issuers to trust.
Device	Enabled	Device authorization allows for manual approval of devices in accordance with RFC 8628. Learn more about device authentication.
Device	Verification URI	The URI used for device authorization. This is the URI the device can use for verification, but doesn't include the user code. This response complies with section 3.2 of RFC 8628.
Device	Usercode verification URI	A verification URI that includes the user code, but is designed for non-textual transmission.
Grants	Access token validity	The duration of time between authentication prompts. Must be equal to or less than the grant validity.

Tab	Field	Description
		Access tokens automatically expire when the grant validity expires. This setting allows you to increase security by requiring periodic authentication to the system. When a token expires, if the access grant is still valid, a user can obtain a new token. Access tokens have a minimum validity period of one minute. They have an effective maximum validity period of the grant validity, since even if access tokens are still valid, once the grant validity expires, no access is granted. Learn more about the terms used on this tab.
Grants	Grant validity	The duration of time that the application will be able to access Venafi Platform. After the grant validity expires, an administrator will need to create a new application. A grant length can exceed the access token validity to require users to confirm their credentials more frequently.
Grants	Refresh enabled	When disabled, the system uses the *grant validity period* as both the *grant validity* and the *access token validity*. When enabled, the system allows the token validity to expire, requiring reauthentication for continued access.
Grants	Revoke if...	Allows you to conditionally revoke the grant if the access token is not used for a specified period of time.
WebSDK	API Statistics	Controls whether statistical information about your API usage is sent to Venafi. These statistics **only** include these three things: ■ The name of the endpoint. ■ The date and time the endpoint was accessed. ■ The duration of time it took for the endpoint to return data to you (if timing is enabled).

Tab	Field	Description
		No sensitive data is accessible to the statistics engine. See our statement on user analytics. Venafi uses this data to help us understand how Trust Protection Platform's APIs are being used so we can target our development efforts in the areas where our customers are using the product. Statistics are collected using a product called Pendo. Their data privacy policies apply in addition to the Venafi Trust Protection Platform privacy policy.
WebSDK	Session cache size	(Called **Session pool size** in the web console.) Specifies the number of concurrent sessions for API calls. If the number of simultaneous API calls exceeds the pool size, the oldest unused session is removed from the pool. Learn more about the terms used on this tab.
WebSDK	Validate/Expire every	The number of minutes each *access token* remains in memory. This functions essentially like a session cache, ensuring callers remain authorized to access the system. The default is five minutes. This field is used in conjunction with the **Validate Grant on Every API Access** setting. If the **Validate Grant on Every API Access** setting is *enabled*, this setting is ignored. If the **Validate Grant on Every API Access** setting is *disabled* (recommended), this setting applies.
WebSDK	Drop inactive sessions after	If a token is not used for this period of time, it is access permission is dropped. When the client reconnects, they will need to authenticate again.

Tab	Field	Description
WebSDK	Refresh user rights every	Determines how often user permissions are validated. While a token may remain valid, a caller's permissions within a scope may have changed. This setting determines how often the system validates these permissions. Longer times are more performant. Shorter times are more secure. The default is five minutes. Learn more about scopes and restrictions.
WebSDK	Validate grant on every API access	When unchecked (normal mode), credentials are cached for a specified amount of time (determined by the **Validate/Expire every** setting, above). When checked (strict mode), credentials are checked on every single API call, which has a measurable decrease in performance.[1] This setting is called **Expiration Mode** in the web console.
WebSDK	Enable API documentation	When you access the documentation on the Trust Protection Platform server in your environment, you can see detailed API documentation in Open API format when you visit the following URL: `https://your-server_url/vedsdk` You can disable is feature if you don't want users to be able to access the OpenAPI version of the documentation at the page listed above. When enabled, you can determine if you want the default viewer to use OpenAPI Epxlorer, Swagger, or ReDoc. Default: enabled, Open API 3.0.

[1]Because this feature queries the database for every API call, internal testing suggests that using strict mode (enabled) can increase call time by around 40%. While this may seem nominal for a single API call, in the aggregate it can dramatically affect performance for all components using the server.

Tab	Field	Description
		If this feature is enabled and users go to the `/vedsdk` URL, they will see the default viewer. However, they can use a different viewer by using an alternative URL. See Testing the Web SDK from the browser.

Revoke User Grants

Applies to the following roles: `Admin` and `Grant Admin`. Application owners need to click on their application in the Client Applications list to revoke user grants tied to their application.

If you want to immediately remove an identity's current grants (but not prevent them from obtaining new grants), use this action to specify which user should have their current grants revoked.

As in all identity fields, you can only see identities from the identity provider your current account is associated with. For example, the local `admin` user can't see active directory users, and a user logged in through active directory as an admin can't see local users.

Using the MMC snapin, you can configure your local machine to connect to your Venafi server using multiple identities at the same time, making it easy to see how different combinations of roles and scopes provide different access.

> **DID YOU KNOW?** You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.
>
> Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

Delete Identity Rules

Applies to the following roles: `Admin` and `Grant Admin`. Application owners need to click on their application in the Client Applications list to delete the rules tied to their application.

If you want to immediately remove an identity's ability to obtain new or refreshed grants, use this action to specify which user should prevented from obtaining any grants.

As in all identity fields, you can only see identities from the identity provider your current account is associated with. For example, the local `admin` user can't see active directory users, and a user logged in through active directory as an admin can't see local users.

> **DID YOU KNOW?** You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.
>
> Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

Using roles for access management in Venafi Configuration Console

When an identity accesses applications through the API, what they can do is determined by the role that is assigned to their identity.

List of oAuth roles

The following table lists the roles used for access management, and what rights they have.

Role	Access details
User	■ Any identity that has not specifically assigned a different role automatically has the User role. The User role cannot be assigned directly.
Auditor	■ Can see everything but change nothing ■ The Auditor role is automatically given to an identity that has Trust Protection Platform auditor rights. It can also be assigned directly to any identity.
Application Maintainer	■ Can modify the properties (such as name, scope, description) of specific applications ■ This role can be assigned by an Admin or by the Application Owner.
Application Owner	■ Can modify and delete applications they own ■ Can modify and delete rules related to applications they own ■ Can revoke grants issued for applications they own

Role	Access details
	■ Can assign and revoke the maintainer role for applications they own ■ Can assign and revoke the owner role for applications they own ■ This role can only be assigned by an Admin.
Mixed Owner/Maintainer	■ Indicates that the user is the Application Maintainer of at least one application and the Application Owner of at least one application. ■ This role cannot be directly assigned but is implied from a user being assigned the Application Owner and Application Maintainer roles.
Grant Admin	■ Can view all applications and rules ■ Can view and revoke all grants for a user ■ This role is intended for users or processes performing off-boarding tasks ■ This role can be assigned by an Admin.
Admin	■ Can create, modify and delete applications ■ Can create, modify and delete rules ■ Can issue and revoke grants ■ Can assign and revoke Application Maintainer and Application Owner roles for any application ■ Can assign and revoke the Admin role ■ Can configure global settings (session parameters, auth parameters, etc.) ■ Any master administrator automatically has this role, but it can also explicitly be assigned to regular identities by an existing OAuth Admin.

Assign a role to an identity

1. Connect to the Venafi Configuration Console on the Venafi server, or use the Venafi Access Management MMC snap-in to connect to the server you want to manage.
2. From the **Venafi Access Management** node, click **Roles**.

3. In the Actions panel, click **Assign...**.
4. Select the role you want to assign.
5. In the **To:** field, locate the user or group to be assigned the specified role.
6. [Conditional] If the new role is `Application Maintainer` or `Application Owner`, select which application this role applies to.
7. Click **OK**.

Revoke a role from an identity

1. Connect to the Venafi Configuration Console on the Venafi server, or use the Venafi Access Management MMC snap-in to connect to the server you want to manage.
2. From the Venafi Access Management node, click Roles.
3. Locate the role you want to revoke.
4. In the Actions panel, click **Revoke...**.
5. [Conditional] If a confirmation modal appears, click **Yes**.

Client Applications

Equivalent functionality

This topic covers the Client Applications node that is part of the Access Management feature in the Venafi Configuration Console and it's associated MMC snap-in.

Equivalent functionality is available in the web console. See "Integrating other systems with Venafi products" on page 752 for more information.

Equivalent functionality is also available in the Web SDK. See OAuth application endpoints for more information.

The Client Applications node allows you to manage your OAuth environment for API connections to Trust Protection Platform to create, update, manage, and delete applications.

Remember that what you can do with an application depends on the role assigned to the identity used to authenticate. See "Using roles for access management in Venafi Configuration Console" on page 396 for details.

The Applications panel lists all client applications in the system. Click on an application to see the Rule list for that application, which is a list of users with information about each user's scope and access.

Depending on your role, you may be able to perform the following actions.

Add a new application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. In the Actions panel, click **Add New Application...**.
3. Use the following table to help you set the required settings.

Order	Name	Description
1	ID	The ID of the application. This ID must be unique. It appears as the **Client ID** on the API Integrations list on the Trust Protection Platform web console, and as the *ID* in the API response.
2	Name	The name of the application.
3	Description	A description for the application.
4	Vendor	The name of the vendor that created the application.
5	Application URL	A URI to learn more about the application.
6	Required Scope	The minimum scope the application requires.
7	Maximum Scope	The maximum scope the application knows to use.
8	Override Global Defaults	Settings in this section are not required. You only need to modify if you want this application to behave differently than the global defaults.
9	Access tokens are valid for	The seconds a token for this application should be valid. Not passing a value uses the system default.
10	Grants are valid for	The seconds a grant for this application should be valid. Not passing a value uses the system default.
11	Grants can be renewed	`true` or `false` to set default behavior grant renewals. Not passing a value uses the system default.
12	Revoke if ... expired for	If an access token is expired and not renewed within the specified time frame, you can revoke the token.

Modify an existing application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Properties**.
4. Modify the application's settings, as desired.

   A table with descriptions for each filed is available in the previous section.
5. Click **OK**.

Add a new rule

Rules show the identities that have been given permission to request a grant for an application, along with what access the identities are allowed.

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Add New Rule...**.

4. Use the following table to help you set up the rule.

Order	Name	Description
1	Application	(Read Only) The application that can request access.
2	Trustee	The identity (user/group) that is allowed access.
3	Description	A description or explanation of the rule
4	Maximum Scope	The maximum scope the application is allowed to request.
5	Access tokens are valid for	The length of timean access token is valid. If this box is not checked, the system default at the time the grant is issued is applied.
6	Grants are valid for	The length of time, in seconds, until the grant expires and can no longer be renewed.If this box is not checked, the system default at the time the grant is issued is applied.
7	Grants can be renewed	If checked, a grant issued under the rule can be renewed. If not checked, it cannot not. If this box is not checked, the system default at the time the grant is issued is applied.

5. Click **Add**.

Delete an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Delete application...**.
4. [Conditional] If prompted, click **Yes** to confirm you want to delete the application.

Delete a single rule for an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.

   Wait for the application's rule list to load.

3. Click on the Rule you want to delete.
4. In the Actions panel, click **Delete rule...**.

Delete all rules for an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Delete all rules...**.
4. [Conditional] If prompted, click **Yes** to confirm you want to delete the application.

About JWT Mappings

A JSON Web Token (JWT; pronounced 'jot') is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. If Trust Protection Platform trusts the certificate used to sign the JWT, it trusts the identity information (claim) provided in the JWT.

JWT mappings are a way to tell Trust Protection Platform which issuers to trust, and how to map identity information in the claim to identities in Trust Protection Platform. This is a crucial part of the authentication process.

In addition to the general JWT mappings, you can also map Active Directory (AD) accounts to a JWT. This involves adding the AD user to the access management API integration and configuring the Access Management Snapin on either an admin's workstation or the TPP server. After these steps, you will be able to map to AD users when setting up a JWT mapping.

JWT Mappings operate in tandem with the central proxy configurations set at the root of the Platforms tree. See "About using an HTTP proxy" on page 784.

Want to know more? Learn about JSON web tokens in this Wikipedia article. Equivalent functionality is available in the WebSDK. See OAuth JWT mapping endpoints for details.

JWT mappings tell Trust Protection Platform which issuers to trust, and how to map identity information in the claim to identities in Trust Protection Platform.

Map AD Accounts to JWT

Mapping Active Directory (AD) accounts to a JWT mapping involves the following steps:

Method 1: Use an Admin's workstation

1. Add the AD user to the access management API integration.
2. Install VenafiMMC.msi on the Admin's workstation.
3. Launch mmc.exe and add the Venafi Access Management Snapin.

Method 2: Use the TPP Server

1. Add the AD user to the access management API integration.
2. Launch mmc.exe on the TPP server.
3. Add the Access Management Snapin.

After following either of these methods, you will be able to map to AD users when setting up a JWT mapping.

Add a new JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. In the Actions panel, click **Add New Mapping...**.

3. Use the following table to help you set the required settings.

Order	Name	Description
1		The name of the application
2		The Issuer URI to be trusted for this mapping
3	(Audience) Field	The name of the JWT field indicating the audience. You can click the Load JWT button if you want to paste in an existing JWT to automatically set these values.
4	(Audience) Must Match	The value that the audience field must match for the token to be accepted.
6	(Subscriber) Field	The name of the JWT field indicating the identity owning the token
7	(Subscriber) Map to	Select an identity for a token issued for this mapping. **NOTE** This field is evaluated as a RegEx (regular expression), not as a string.
8	(Subscriber) Extract identity	The regular expression to use to obtain the identity from the Subscriber Field. The first group matching the expression is used to determine the identity.

4. Click **Add**.

Edit an existing JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. Click on a JWT mapping in the list.
3. In the Actions panel, click **Properties**.
4. Modify the JWT's mapping settings, as desired.

   A table with descriptions for each filed is available in the previous section.
5. Click **OK**.

Delete a JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. Click on a JWT mapping in the list.
3. In the Actions panel, click **Delete...**.
4. [Conditional] If a confirmation modal appears, click **Yes**.

Common terms in access management

Throughout the documentation we use the following terms when discussing the concept of access management for API applications.

Grant / Access Grant

A grant represents the right to access a resource URL (such as WebSDK, VedHSM). A grant can have limited lifetime, depending on configuration (default is one year), and a grant has attached to it what application is allowed to use it, and what scope for that application was granted. A grant is issued by the authentication server in exchange for valid credentials.

The Venafi Configuration Console and API use the term **grant**. The web console uses the term **access grant**. These terms are interchangeable.

Access Token / Token

OAuth uses bearer tokens for API authentication. The authentication server will return one or more tokens as part of an issued grant. Tokens infer access rights, and have a (configurable) limited lifetime. See the Auth REST for token management section for more information about getting tokens.

The Venafi Configuration Console and API use the term **access token**. The web console uses the term **token**. These terms are interchangeable.

Refresh Token

A refresh token might be supplied as part of the grant returned by the authorization server, if configured. Access Tokens have limited validity, and to ensure they don't get too much exposure, they often expire before the grant expires. In that case, a refresh token will have been provided when the grant was issued, and this refresh token can then be used to obtain a new access token (and a new refresh token).

Application (Integration)

Before an application can request a token, the application must be registered with the server. Unknown Client IDs/Applications cannot request grants.

In theTrust Protection Platform web console, Applications and Application IDs are referred to as *Integrations* and *Client IDs*.

Applications can be created in the web console from the API Integrations Inventory.

Scope

To allow fine-grained control over what operations an application is allowed to perform, each API endpoint requires a particular scope, and when requesting a grant, an application indicates what scope it requires. This allows you to restrict risk even if the user credentials used to obtain the grant provide wider permissions.

The scope controls what category of endpoints may be accessed. For example, `certificate` or `ssh`, or `statistics`.

Learn more about what scopes and restrictions are available.

Restrictions and Privileges

Within a scope, the caller is explicitly given the ability to do certain actions based on their privileges and restrictions.

If no privileges and restrictions are given for a particular scope, the caller will have *read* access to the related endpoints.

For example, a caller with the scope of certificate and no privileges and restrictions will be able to read certificate data, but will have no ability to take any actions. For the certificate scope, a caller can be given any combination of the following privileges and restrictions: **approve**, **delete**, **discovery**, **manage**, and **revoke**.

Other scopes have their own list of privileges and restrictions that can be granted for an identity.

Learn more about what scopes and restrictions are available.

Session cache size

You can limit the number of active sessions by setting the session cache size. In the web console, this is also called **session pool size**. When the cache size reaches it's limit, the oldest sessions are removed. A caller would need to refresh their token to access the application again.

Credentials

To obtain a grant, the authentication server requires credentials. The authentication server can be configured to accept any of the following as valid credentials:

- Username/Password
- User Certificate (The identity for the grant is obtained from the certificate)
- Windows Authentication (NTLM/Kerberos)
- Json Web Token (JWT) (The identity for the grant can be obtained from the JWT or be a fixed identity, based JWT contents)
- Device (unauthenticated request that requires manual approval)

Code Signing

Global code signing configuration is done in the **Venafi Code Signing** node. While this node appears for everyone, it is active only for those who have licensed Venafi CodeSign Protect.

> **DID YOU KNOW?** The Code Signing node can be run as an MMC Snap-in on standalone Windows workstations. For more information, see "Venafi MMC Snap-In Collection" on page 361.

The Code Signing page has a **Summary** section that shows some high-level statistics about your code signing configuration. Click a number from the **Summary** section to be taken to that section in Venafi Configuration Console.

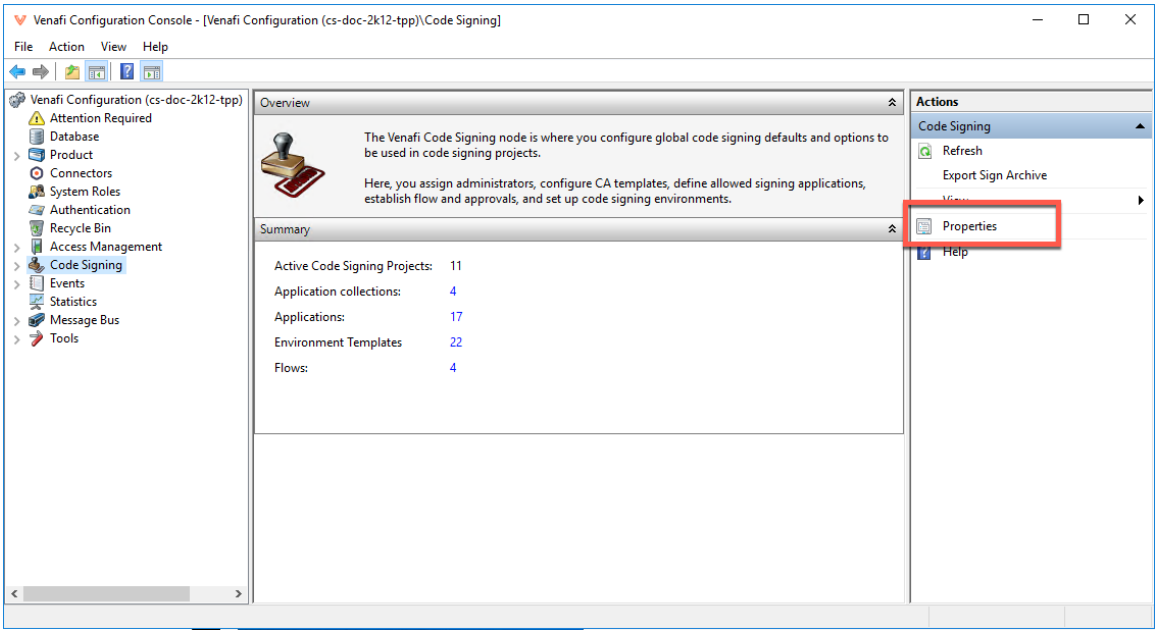
From this node, you can also set global code signing defaults and restrictions. For additional instructions, see "Set global code signing properties" below.

For additional information and instructions, see Configuring global Venafi CodeSign Protect settings in the *Venafi CodeSign Protect Guide*.

Set global code signing properties

There are a number of properties that Code Signing Administrators can set at the global code signing level. Some of these properties serve as defaults that can be overridden in Environment Templates, whereas others become restrictions that cannot be overridden. To access these settings, select the Code Signing

node in the Venafi Configuration Console, and in the Actions Panel, click **Properties**.



The **Code Signing Properties** window opens. The window is divided into the following tabs:

- "Global Code Signing Configuration tab" below
- "Default Flows tab" on page 175
- "Request Identifier Fields tab" on page 178

Global Code Signing Configuration tab

Default Containers

In this section, you can set the default storage locations for **Certificate Authority Templates**, **Credentials**, and **Certificates**. To change any of these locations, click the drop-down box and select a new folder.

These locations can be reset in the Environment Templates.

Private Key Generation and Storage

This section lists the available generation and storage locations for code signing private keys. Place a checkmark next to each location you want to use for key storage. The storage locations selected here will be the only locations available in the Environment Templates.

NOTE If you do not have any connected HSMs, then the only option shown is **Software**, which is the Trust Protection Platform Secret Store. To select an HSM, you first need to configure an HSM. See "Creating a HSM connector" on page 562 for instruction on connecting an HSM.

Options

- **Key Users may not have other roles in the same project**. Checking this box restricts users assigned as Key Users or members of a Key User group from having any other role on the code signing project.

  NOTE User roles in the project are checked when the key is used, not when the project is created or edited. The reason for this is that group membership is dynamic, which means that the only reliable time to validate user roles is at the time of key use.

  NOTE The Trust Protection Platform Master Admin and Code Signing Administrator roles cannot be assigned as CodeSign ProtectKey Users.

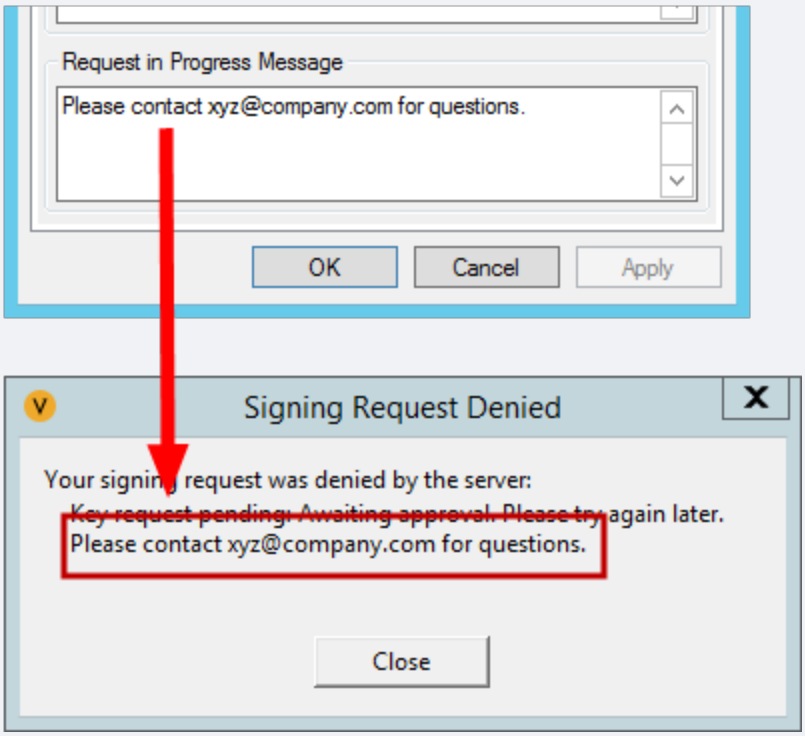
- **Role members must be in groups**. Checking this box disallows Owners from selecting individual users to fill roles in code signing. All roles must be assigned to groups.

- **Wait period before timing out requests**. Specifies the number of seconds to wait before the CSP will time out. This value is pushed from the Trust Protection Platform server to the CSP clients.

Request in Progress Message

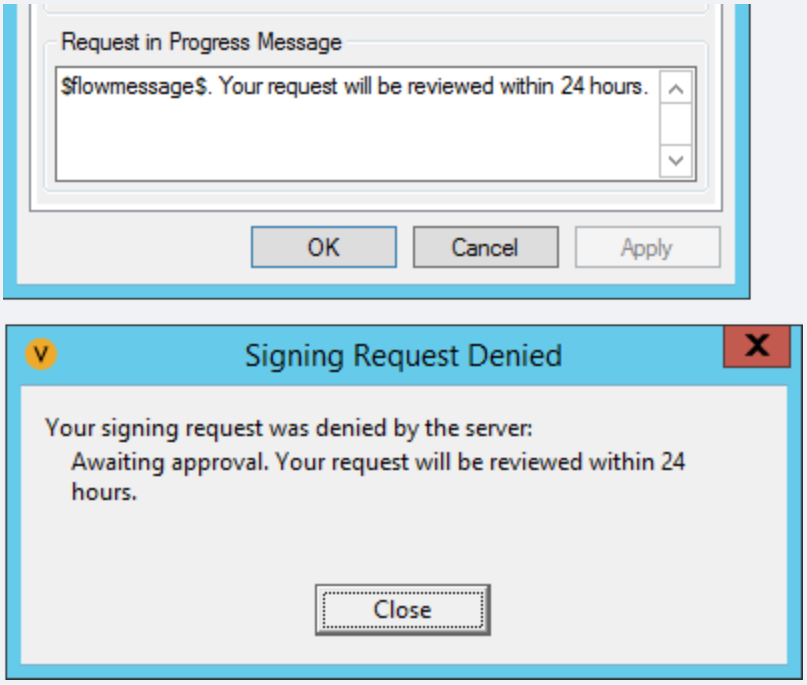
The **Request in Progress** field provides Code Signing Administrators the ability to customize the dialog returned to the Key User when an approval is required or a signing operation is rejected.

EXAMPLE In the case where approval is required to use a code signing key, providing an email address for Key Users to get additional information may be helpful.



If you enter a message that contains the macro "$flowmessage$", only what you enter will be displayed, with "$flowmessage$" being replaced with the flow status.

EXAMPLE Using the "$flowmessage$" macro.



Signing archive options

Details about code signing events are saved in the code signing archive, which you can search either in the CodeSign ProtectUI or through the audit API endpoints. By default, archive events are never deleted.

To delete archive events that are older than a set period, adjust the value in the **Keep Sign Archive Entries for *xx* days** field.

WARNING! All archive entries older than the number of days you set will be deleted.

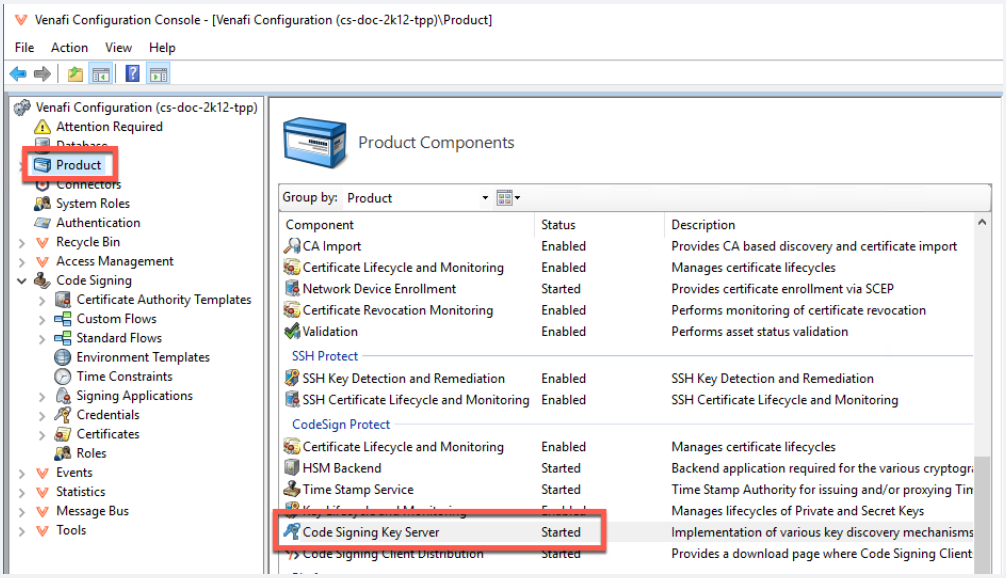
To keep CodeSign Protect from creating new archive entries altogether, select the **Disable Sign Archive** checkbox. When the archive is disabled, any existing entries will remain in the archive, even if they exceed the period set using the **Keep Sign Archive Entries** option.

If the signing archive is currently disabled, you can enable it by deselecting the **Disable Sign Archive** checkbox.

Disable JWK Public Keyserver

Starting the Code Signing Key Server component enables a JWK public key server and a GPG public key server. Checking the **Disable JWK Public Keyserver** checkbox disables the JWK key server but leaves the GPG key server active.

NOTE You can check if the Code Signing Key Server component is started by clicking the **Product** node in Venafi Configuration Console and scrolling down to the CodeSign Protect section.



Certificate Configuration

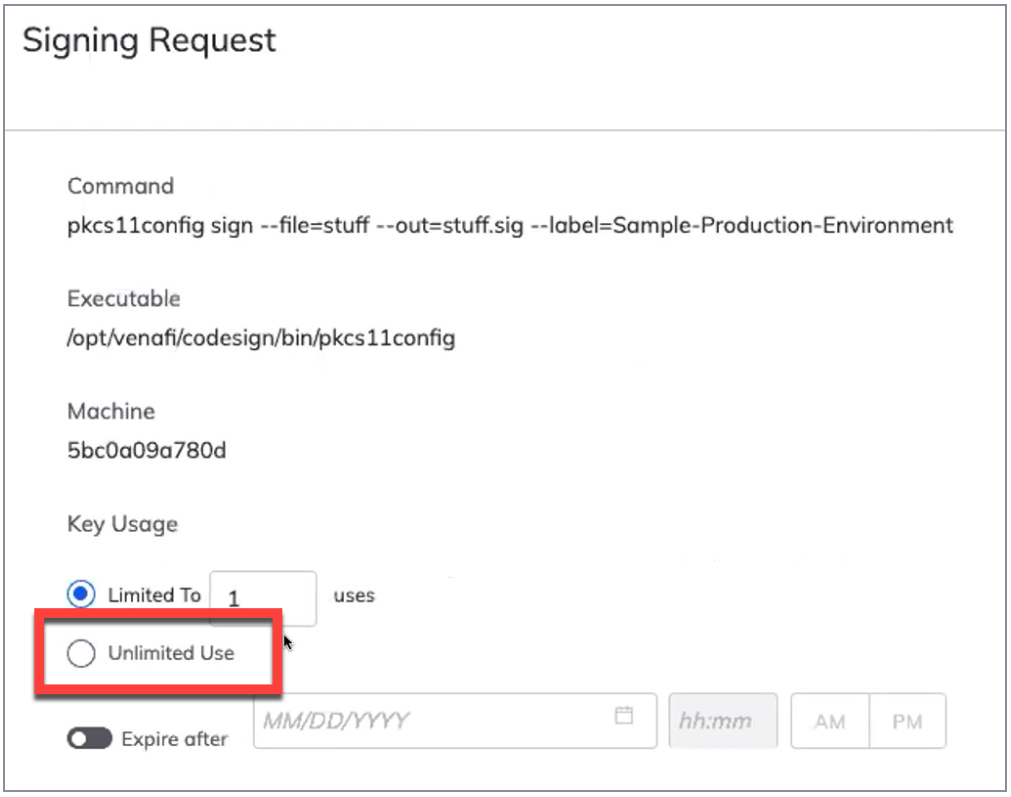
If you want Owners to be able to add a SAN Email to certificate requests, check the **Allow SAN Email** checkbox.

Default Flows tab

Signing Flows

To remove the option for Key Use Approvers to allow unlimited signings when approving a signing request, check the **Approvers may not allow unlimited signings upon signing request approval** checkbox in this section. With this checked, the **Unlimited Use** radio button (outlined in the screenshot below) will be removed from the Signing Request approval screen entirely.

If you leave Unlimited Use enabled, Key Use Approvers will be required to select a date and time when the unlimited key use approval expires.



Create, Update, and Delete Flows

The Create, Update, and Delete sections specify the Flows invoked when certain actions are taken on a Project or Environment.

By default, the Flows that are assigned require no approvals. If you want to add approval steps for any of the actions explained below, you'll need one or more Change Management Flows with the approval settings you want.

> **EXAMPLE** Suppose you wanted to enforce Code Signing Administrator approval anytime a new Environment is added or deleted, and Project Owner approval anytime an existing Environment is changed. You also want a Code Signing Administrator to have to approve Project deletions.
>
> First, you'd create two Change Management Flows–we'll call those Flows "Administrator Approval" and "Owner Approval." The Administrator Approval Flow would have an "Administrator" approval action, and the Owner Approval Flow would have a "Standard" approval action with the **Attribute** set to Owner.
>
> Next, you assign the Flows in the Default Flows tab of Global Code Signing properties. For Create and Delete, you assign the Administrator Approval Flow. For Update, you assign the Owner Approval Flow.

If you want to use Flows that enforce approvals, and those Flows aren't in place yet, start by creating them. Once they are in place, return here to assign them. You can assign Flows by clicking the drop-down selector for any of the options described below, and then selecting the Flow.

Create

The **Create** section sets the Flow that is invoked anytime an Environment is added to a Project. This Flow is invoked no matter what state the Project itself is in. If the Flow requires approvals, the Environment will be in the *Disabled* status until the approval is given. Once approved, it moves to the *Enabled* state.

If the Create Flow requires approvals, approvers will be notified anytime a new Environment is added to any Project. Approvers should follow the instructions in Approving or rejecting changes to CodeSign Protect Environments to take action on the request.

Update

The **Update** section sets the Flow that is invoked anytime an existing Environment is changed. This Flow is invoked no matter what state the Project itself is in. If the Flow requires approvals, the Environment remains *Enabled* in its original configuration while awaiting approval. Once the approval is given, the updates to the Environment take effect.

If the Update Flow requires approvals, approvers will be notified anytime a new Environment is added to any Project. Approvers should follow the instructions in Approving or rejecting changes to CodeSign Protect Environments to take action on the request.

Delete

The **Delete** section sets the Flows that are invoked anytime an Environment or a Project is deleted. If the Flow requires approvals, approvers will be notified anytime a Project or Environments deletion request is received. Approvers should follow the instructions in Approving or Rejecting a project deletion request to take action on the request.

When an Environment is deleted, it remains in the *Enabled* state until the deletion is approved. Once approved, the Environment, its associated certificates, and keys are deleted.

When a Project is deleted, it is put in the *Pending Deletion Approval* state. In this state, none of the Environments are enabled. Once the deletion is approved, the Project and all its Environments are deleted.

Request Identifier Fields tab

The **Request Identifier Fields** options allow Code Signing Administrators to determine which attributes of a signing request are used to match previous signing requests that are not yet complete. These global settings can be overridden in Environment Templates.

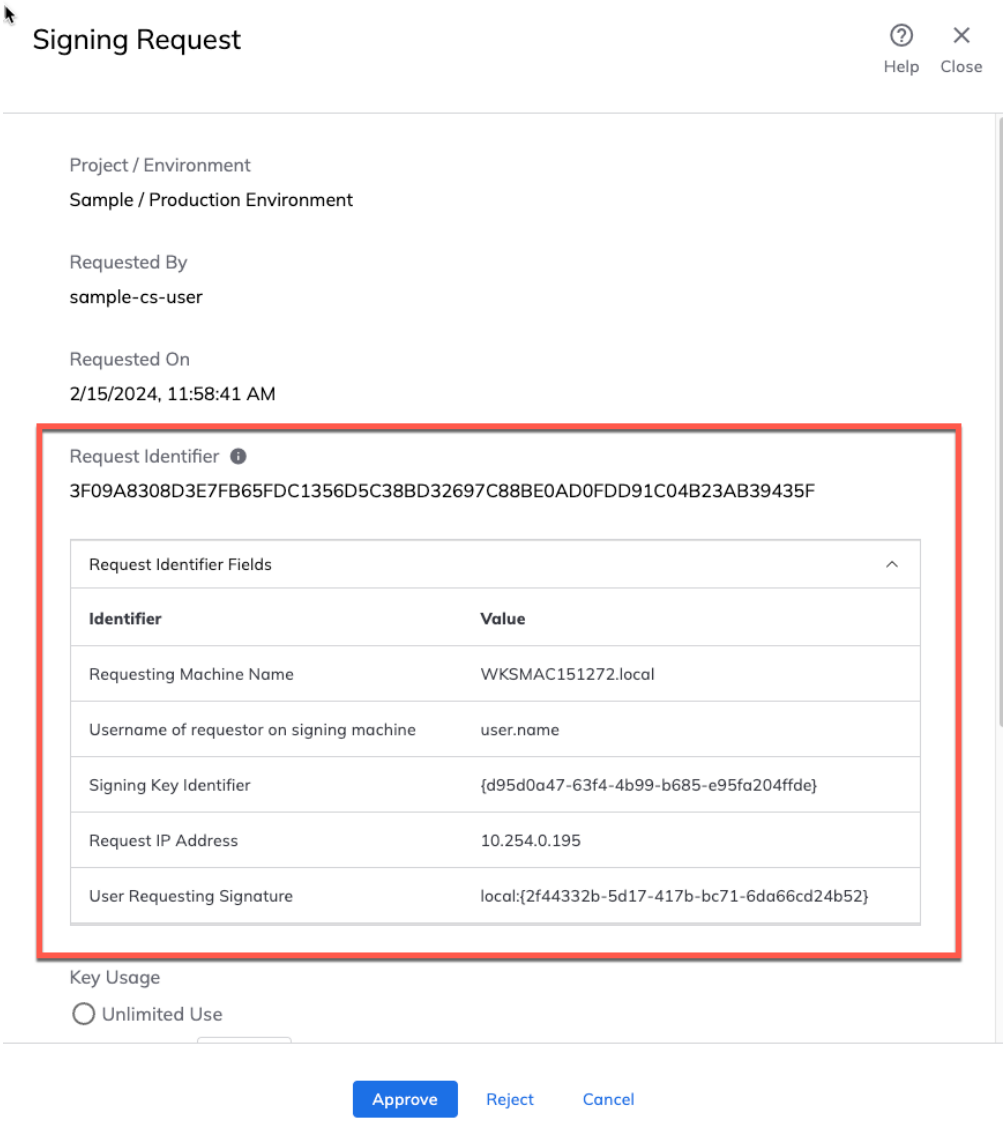
Learn more about how request identification works

Every code signing private key managed by CodeSign Protect is associated with an Environment, and each Environment has an associated Flow. The final step in every Flow is to sign the code. In some cases, a signing request's Flow cannot finish in a single operation, such as in the case of a required approval.

When you submit a signing request, the values from the request identifier fields are hashed to create a unique request identifier. This request identifier is used to determine if the request is a new request or a continuation of a previous request that is awaiting approval.

If the identifier doesn't match any existing identifier for requests in the Pending Approval or Active Approval states, it is considered a new request and will start at the beginning of the Flow that is associated with the Environment. If the identifier does match an existing identifier, then it is considered a continuation of an existing request.

When a Key Use Approver approves a signing request, they will see both the request identifier as well as the request identifier fields, as shown in the screenshot below:



To learn more about Flows, see "Create Flows" on page 196.

The following values can be used to match signing requests with previously-submitted requests that are not yet fulfilled. By default, the following fields are selected:

- Command Line
- Signing Key Identifier

- Requesting Machine Name
- Username of requestor on signing machine

CAUTION Changing these options invalidates any existing pending approvals.

Identifier	Description
Command Line	The actual command used to issue the signing request. This is enabled by default. This identifier should be disabled for GPG Environment Templates that use a Flow with approvals.
Signing Executable	The filename of the signing application.
Signing Executable Checksum (Hash)	The hash of the signing application being used to sign.
Signing Executable Signer	The signer of the signing application. This is the subject of the certificate used to sign the signing application itself.
Signing Executable Size	The disk size of the signing application.
Request IP Address	The IP address of the workstation from which the request was issued.
Request Justification	The request justification is a freeform field that allows the Key User to include a reason why they are requesting use of the key.
Signing Key Identifier	The Trust Protection Platform unique identifier for a private key. This is enabled by default.
Requesting Machine Name	The name of the workstation from which the signing request is made. This is enabled by default.
Data to be signed	The hash of the data (such as an executable, macro, or document) that the signing application creates. **NOTE** Checking this option ensures that the binary being signed cannot change between the request, approval, and signature.
User requesting signature	The Trust Protection Platform username of the user requesting the signing.
Username of requestor on signing machine	The workstation username of the user requesting the signing. This is enabled by default.

Create Certificate Authority (CA) templates

Each environment in a code signing project must have a CA template assigned to it. Those CA templates are defined using the steps defined in this section.

The following Certificate Authorities are supported with CodeSign Protect:

- Adaptable CA
- DigiCert
- Entrust Certificate Service
- Microsoft CA
- Microsoft CA Pool
- Out-of-band CA
- Self-signed CA

Create an Adaptable CA template

An Adaptable CA can be used in place of a CA or application driver that does not yet exist or in place of a supported driver requiring advanced and tighter integration. For more information, see Adaptable CA.

To create and configure a new Adaptable CA template object

1. Access Venafi Configuration Console.
2. From **Venafi Code Signing (TPP Code Signing)** > **Certificate Authority Templates**, click **Create**, and then select **Adaptable CA Connector**.
3. Specify a name for the new CA template. This name displays when adding a CA template to an Environment Template.
4. Click **Create**. The **Configure New Connector** screen displays.
5. Refer to the following table to configure the connector:

Field	Description
Description	Enter a description that describes the purpose of your new job. A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
Contact	Select one or more users to be contacts.
Username Credential	Select an existing credential or create a new credential by selecting a container.
Certificate Credential	If your organization requires two-factor authentication, then select both a user name credential and a certificate credential.
Secondary Credential	If you need to select another credential, then from the Secondary Credential property, select a user name, certificate, password, or CyberArk credential object. **TIP** Use this option to avoid having to hard code additional credentials in your script or having to utilize other solutions outside of Trust Protection Platform.
Service Address	Type the URL, FQDN, or IP address of your certificate authority API, according to how you've implemented this in your PowerShell script. For example, https://domain.net, subdomain.domain.org, 123.456.1.2, or localhost. Specifying the URL of your CA's API lets you use the same script to target different instances of the same CA vendor product. So this option is primarily applicable to CAs that are not available on the public Internet because those service addresses are the same for every customer. **TIP** Unless you're developing and testing a PowerShell script, configuring **Service Address** or **Profile String** (below) is typically not something you'll need to do. The primary benefit of these settings is for third-party Venafi partners, enabling the PowerShell scripts they provide to be used as-is without customers having to customize them. A secondary benefit is that in the event that service URL or configuration changes are made, the values you specify are passed to every PowerShell function in your scripts automatically, preventing service interruptions and avoiding the need to update or re-validate your PowerShell scripts. For more information, see Preventing PowerShell script updates following service URL changes.
Profile String	Type the profile string used by your PowerShell script.

Field	Description
	Specifying a certificate product, profile, or template lets you use the same script for different types of certificates supported by the target CA. This setting works with **Service Address** and depends on your script. For example, your script might reference the name of an identifier, a certificate product, profile, or template (e.g. x456-5424454:ssl_private:25423g-542352-2463). **TIP** This field is designed to provide flexibility to your implementation of a PowerShell script. If you're implementing the script, it's important that you verify the value specified is valid and uses the required syntax.
PowerShell Script	Select your Windows PowerShell script from the PowerShell Script list. Only scripts contained in the Program Files\Venafi\Scripts\AdaptableCA folder appear in this list. If the script you want to use isn't listed, verify it has been placed into the correct directory on your Trust Protection Platform server. See About the Adaptable CA PowerShell script.

Field	Description
Renewal Window (days)	Specify how many days prior to the expiration of an existing certificate that the certificate should be renewed. Any certificates falling outside the renewal window are handled through a replacement or re-issuance.
Allow Reissuance	Enables renewal without changing the original expiration date.
Subject Alt Name Enabled	In X.509 certificates, a Subject Alternative Name extension allows a certificate subject to be associated with the service name and domain name components of a DNS Service Resource Record. See About Subject Alternative Names (SANs).

Field	Description
When script is updated, fix related certificate errors	Enables Trust Protection Platform to fix certificates affected by changes to the associated PowerShell script. For more information about how changes to scripts can affect certificate enrollment, see Protecting against unapproved changes to Adaptable CA scripts.
Enable Debug Logging	Logs debug information to enhance troubleshooting capabilities. For information about how enabling this option works with the PowerShell script, see About debug logging in the Certificate Authority and Hosting Platform Integration Guide.
Custom Fields	Data related to the custom fields you select are passed using functions defined in the PowerShell script. See "Working with custom fields" on page 891.

What's next?

After you create a CA template object, you can use it in setting up CodeSign Protect by following instructions at Administrator setup

in the Code Signing Guide.

Create a DigiCert CA template

A DigiCert CA template requires an API credential. If you haven't created a DigiCert credential yet, this procedure provides instructions on how to do that. Have your DigiCert API key ready before beginning this procedure.

1. From the Certificate Authority Templates node in Venafi Configuration Console, click **Create**, and then select **DigiCert CA Connector**.

2. Give the new CA template a name. This is the name that will be shown when adding a CA template to an Environment Template. Click **Create**. The **Configure New Connector** dialog opens with the **Settings** tab selected.
3. Enter a **Description** for this template.
4. From the **Contact** drop-down list, select a contact.
5. The **API Key** drop-down list allows you to select the credential to use for this template. The credential verifies your identity with DigiCert and is needed to be able to complete the rest of this template.

   If the credential you want to use for this template already exists, you can select it. If not, you'll need to create a new credential. Both procedures are documented here.

   ### To create and use a new credential

   Have your DigiCert API key ready before starting this procedure

   a. Click the **API Key** drop-down.
   b. Click the **Location** drop-down.
   c. Click **Create**.
   d. Enter an **Object Name** that will allow you to easily identify this credential. Optionally a **Description** and **Contact** for this object, and click **Create**.
   e. In the **API Key** field, enter your DigiCert API key. Optionally, enter a **Description** and select a **Contact**.
   f. Click **Save**.

   ### To use an existing credential

   a. Click the **API Key** drop-down.
   b. Click the **Location** drop-down.
   c. If you know the name of the credential, enter the name and click **Search**. If you do not know the name, enter * and click **Search**.
   d. Click the credential, and then click **Select**.
   e. Click **Save**.

6. Refer to the following table to complete the remaining CA template settings:

Field	Description
Product Name	Select from the list of products available based on the API Key used to authenticate to the DigiCert CA.
Organization	Select the organization licensed to use the DigiCert product.
Signature Algorithm	Lets you select the algorithm DigiCert uses when signing a requested certificate. You must select one of the following supported signature algorithms: ◦ SHA256 (default) ◦ SHA384 ◦ SHA512
Org Unit Override	(Optional) Type one or more OU values to submit to DigiCert with the CSR to override the OUs specified by policy or in the CSR. You must enter one OU value per line. If no organizational unit override values are specified on the CA template, then the OUs specified on the CSR are submitted to DigiCert with the CSR.
Validity Period	Assign a validity period to be used when enrolling certificates. Options include 90 days, 6 months, and 1 year (default). **TIP** If you need to define multiple validity periods, create additional CA objects that differ only in the validity period assignment.
Renewal Window (days)	Specify the number of days before expiration that you plan to renew certificates. The default renewal window is 32 days for all newly created DigiCert templates. Typically, 30 to 90 days ensures sufficient time for all the necessary approvals and processes to be completed so that the renewed certificate is in place before the old certificate expires. You must select a value that is greater than 0 and less than (or equal to) 365 days.

Field	Description
Manual Approval	Requires manual approval for all CSRs submitted using the current CA Template object. When you enable Manual Approval, the administrator must log in to the DigiCert CertCentral CA service and manually approve the renewing certificate.
Allow Reissuance	Lets you reissue certificates so that you can add SANs to existing certificates without wasting certificate units or incurring unnecessary charges.
Allow Users to Specify End Date	The Allow Users to Specify End Date option lets users specify expiration (end) dates for certificates requested from the CA so that they do not expire during your known freeze periods. Typically, renewing certificates that expire during freeze periods requires a more challenging approval process. Setting expiration (or end) dates that fall outside of freeze periods avoids potential interruptions. When a specific end date has been specified, the issued certificate has that date as its expiration date. This check box is cleared after successful enrollment (so that the validity period takes effect thereafter).

Click **OK**.

Create an Entrust Certificate Services Connector

A Entrust CA template requires both a certificate credential and a username credential. If you haven't yet created these credentials, this procedure provides instructions on creating them.

1. From the Certificate Authority Templates node in Venafi Configuration Console, click **Create**, and then select **Entrust Certificate Service CA Connector**.
2. Give the new CA template a name. This is the name that will be shown when adding a CA template to an Environment Template. Click **Create**. The **Configure New Connector** dialog opens with the **Settings** tab selected.
3. Enter a **Description** for this template.
4. From the **Contact** drop-down list, select a contact.
5. The **Certificate Credential** drop-down list allows you to select the certificate credential to use for this template. The credential verifies your identity with Entrust and is needed to be able to complete the rest of this template.

If the certificate credential you want to use for this template already exists, you can select it. If not, you'll need to create a new credential. Both procedures are documented here.

To create and use a new credential

Have your Entrust certificate ready before starting this procedure

a. Click the **Certificate Credential** drop-down.

b. Click the **Location** drop-down.

c. Click **Create**.

d. Enter an **Object Name** that will allow you to easily identify this credential. Optionally a **Description** and **Contact** for this object, and click **Create**.

e. Click **Import Certificate**. Select the Entrust certificate to use for this credential.

f. Enter the certificate **Password**. Optionally, enter a **Description** and select a **Contact**.

g. Click **Save**.

To use an existing credential

a. Click the **Certificate Credential** drop-down.

b. Click the **Location** drop-down.

c. If you know the name of the credential, enter the name and click **Search**. If you do not know the name, enter * and click **Search**.

d. Click the credential, and then click **Select**.

e. Click **Save**.

6. In addition to a certificate credential, Entrust requires a username credential.

To create and use a new credential

Have your Entrust username and password ready before starting this procedure

a. Click the **Username Credential** dropw-down.

b. Click the **Location** drop-down.

c. Click **Create**.

d. Enter an **Object Name** that will allow you to easily identify this credential. Optionally a **Description** and **Contact** for this object, and click **Create**.

e. Enter the **Username** and **Password** to use for this credential. Optionally, enter a **Description** and select a **Contact**.

f. Click **Save**.

To use an existing credential

a. Click the **Username Credential** drop-down.

b. Click the **Location** drop-down.

c. If you know the name of the credential, enter the name and click **Search**. If you do not know the name, enter * and click **Search**.

d. Click the credential, and then click **Select**.

e. Click **Save**.

7. Refer to the following table to complete the remaining CA template settings:

Field	Description
Client	Name of your client. This name is used to generate the certificates.
Template	List of supported Entrust SSL certificate templates. Select the code signing certificate to use for this CA template.
Signature Algorithm	Specifies the algorithm that will be used by Entrust when it signs a requested certificate.
Enhanced Key Usage	Value is set by the Template.
Transparency	Value is set by the Template.
Validity Periods	Allows you to control which Validity Periods can be selected. The Validity Period is the period of time (in years) that the certificate is valid.
Renewal Window	A renewal window is the time period before a certificate's expiration date during which a certificate can be renewed. The default renewal window is 32 days for all newly created Entrust templates.

Field	Description
	This option lets you specify the maximum number of days prior to the certificate's expiration date that Trust Protection Platform should treat as a renewal request. If the number of days remaining in the validity period of the certificate is greater than your renewal window setting, then certificate renewal requests are processed as *reissuance* requests. When there is no existing certificate, a new certificate request is submitted to the CA as a new (first time) request. **TIP** You can set the renewal window to a maximum of 364 days; the default setting is 90 days. But the renewal window does not *prevent* you from renewing a certificate that is not yet within the renewal window. Instead it allows you to obtain a replacement version of a certificate when it is not close to expiring while keeping the same expiration date.
Enroll using client's default organization	Enable this option when you want to ensure that CSRs that specify an organization other than the primary (or default) organization—or the organization value associated with your Entrust account—are successfully enrolled and the organization in the resulting certificate is your default organization. For example, if the name of your organization were MajorCo, Inc. and you submitted a CSR with O=*Minor*Co, Inc.—the name of your subsidiary—it would be enrolled successfully but the issued certificate would show O=*Major*Co, Inc. **DID YOU KNOW?** Most public CAs ignore some information in a CSR that is typically already known, such as the city, state and zip code, because they are fixed values of the Entrust customer and already known. This can also be true of the default organization value; however, some businesses have multiple organizations (e.g. through acquisitions, etc.). So in cases where the organization specified in a CSR matches the Entrust customer's default organization, Trust Protection Platform would pass that value to the CA. However, if the specified organization did not include a valid organization in the CSR, it would not enroll. This new option helps to ensure successful enrollment.
Manual Approval	Requires manual approval for all CSRs submitted using the current CA Template object. When you enable **Manual Approval**, the administrator must log in to the Entrust Certificate Services CA service and manually approve the renewing certificate.
Allow Reissuance	Lets you reissue certificates so that you can add SANs to existing certificates without wasting certificate units or incurring unnecessary charges.

Create a Microsoft CA template

1. From the Certificate Authority Templates node in Venafi Configuration Console, click **Create**, and then select **Microsoft CA Connector**.
2. Give the new CA template a name. This is the name that will be shown in Aperture when adding a CA template to an environment. Click **Create**. The **Configure New Connector** dialog opens with the **Settings** tab selected.
3. (Optional) Enter a **Description** and select a **Contact** for this template.
4. Refer to the following table to complete the remaining CA template settings:

Field	Description
Hostname	IP Address or DNS name of the Microsoft CA server. Trust Protection Platform supports both IPv4 or IPv6 connections.
Service Name	Name of the Microsoft CA service. This will match the Common Name (CN) of the CA's certificate.
Credential	User name credential required to connect to the Microsoft CA. This account must have Read, Issue and Manage Certificates, Request Certificates permission on the CA. If this is an Enterprise CA, the account also requires Read and Enroll permissions applied to any templates that TLS Protect will use. The credential can be expressed in any of the following formats, although the format you use depends upon your Active Directory environment: ◦ SAM account name ◦ Domain name syntax (domain_name\username) ◦ User Principle Name syntax (valid_user@orgUnit.domain.com) **To use an existing credential** a. Click the **Credentials** drop-down.

Field	Description
	b. Click the **Location** drop-down. c. If you know the name of the credential, enter the name and click **Search**. If you do not know the name, enter * and click **Search**. d. Click the credential, and then click **Select**. e. Click **Save**. **To create and select a new credential** a. Click the **Credentials** drop-down. b. Click the **Location** drop-down. c. Click **Create**. d. Enter an **Object Name** that will allow you to easily identify this credential. Optionally a **Description** and **Contact** for this object, and click **Create**. e. Enter the **Username** and **Password** to use for this credential. Optionally, enter a **Description** and select a **Contact**. f. Click **Save**.
Template	The Microsoft CA template that you want to associate with the current CA Template object. Trust Protection Platform references this template when it submits the CSR. The template menu is automatically populated when you click **Retrieve**. If new templates are added to the CA, you must click **Retrieve** to update the list of available templates. The template referenced by Venafi's Microsoft CA template object must be configured to have its Subject Name supplied in the request.
Manual Approvals	Requires manual approval for all CSRs submitted using the current CA Template object.

Field	Description
	When you enable **Manual Approval**, the administrator must log in to the Microsoft CA service and manually approve the renewing certificate.
SAN Enabled	Configures the current CA template object to support CSRs with DNS-based subject alt name (SAN) values. **NOTE** DNS SANs are included in the Unified Communications Certificates that are used with Microsoft Exchange 2007 and Microsoft Office Communications Server. If you do not select this option, the current CA template object will not accept CSRs with SAN values. If Trust Protection Platform attempts to submit a CSR with SAN values, the CA Template object returns the following error: `Stage 400 (Creating CSR) SubjectAltName not supported by Application and CA.` **IMPORTANT** Before selecting this option, you must also verify the SAN feature is enabled on your CA engine. It it isn't, the CA returns the same error message when Trust Protection Platform attempts to submit a CSR with SAN values.
Include CN in SAN	Makes it so that every certificate enrolled using the CA template will have the its Common Name included as a DNS Subject Alternative Name (SAN). As of v1.1.7 of the CA/Browser Forum Baseline Requirements, usage of the Common Name is considered deprecated and to be represented instead by an equivalent DNS SAN.

Create a Microsoft Pool template

If you are using two Microsoft CAs, you can configure a Microsoft CA Pool template to automatically enroll certificates using a second CA in the event that the first CA is not successful. There is no functionality today built into Active Directory Certificate Services (ADCS) that provides redundancy in the event of service degradation.

DID YOU KNOW? The Microsoft CA Pool is a special type of CA template. Whereas all other Venafi CA templates define *how Trust Protection Platform interacts with a specific CA and what type of certificates are issued*, the Microsoft CA Pool does neither, but is instead an aggregation of multiple MSCA templates.

So what happens if the first CA fails? In the event that the first Microsoft CA in the CA pool is not available, Trust Protection Platform stops querying that CA for 60 minutes and automatically queries the second CA in the CA pool. This process is repeated up to the optional third Microsoft CA.

TIP Before you create your Microsoft CA Pool template, you should already have at least two MSCA templates defined because you'll need to select them as part of this procedure.

To create a Microsoft CA Pool template object

1. From the Certificate Authority Templates node in Venafi Configuration Console, click **Create**, and then select **Microsoft CA Pool Connector**.
2. Enter a name for this template.
3. Click the **CA Template 1** drop-down. In the Search box, enter the name of the certificate you want to add to the pool, and then click **Search**. Click the certificate to highlight it, and then click **Close**.

   NOTE Rather than searching for a specific certificate, you can use the asterisk * in the search bar to show all available certificates.

   Repeat this step for the **CA Template 2** and (optionally) **CA Template 3** drop-downs.
4. Select the **Manual Approvals** and **Allows Users to Specify End Date** check boxes to enable them.

   IMPORTANT Whether you leave these settings disabled (which is the default setting), or whether you enable them, note that how you set them here overrides the same settings found on the individual MSCA templates you assign to the pool.

   For example, if you have *enabled* Manual Approvals on any of the MSCA templates you include in the pool but then *disable* Manual Approvals here in the Microsoft CA Pool settings, Manual Approvals will be disabled when that template is used by your Microsoft CA Pool.
5. When you're finished, click **OK**.

Create an out-of-band CA template

You can set up an out-of-band CA template so you can use your preferred Certificate Authority (CA), such as Sectigo CA or Apple CA, even if it has a difficult interface with other systems. Or for situations where a CA must transfer Certificate Signing Request (CSR) files and notifications across an air-gapped system.

Using an out-of-band CA connector gives you the ability to transmit CSR files and notifications via email. And keys are stored on and can be downloaded from Venafi Web Console. Also, you can store private keys on a hardware security module (HSM).

Out-of-band CA is an option for single-user environments only. Support for per-user environments coming soon.

To create and configure an out-of-band CA template object

1. From the **Certificate Authority Templates** node in Venafi Configuration Console, click **Create**, and then select **Out-of-Band CA Connector**.
2. Give the new CA template a name. This is the name that you'll see when you're selecting a CA template in the Venafi Web Console. Click **Create**. The **Configure New Connector** dialog opens.
3. In the **Settings** tab, enter a **Description**, and then choose a **Contact** for this template.
4. Enter an **Email Address** to use for sending CSR files and future notifications.
5. Check **Email Certificate Contacts** to send notifications to all contacts, such as Project Owner, specified on the certificate object.

What's next?

After creating a template, you can continue configuring CodeSign Protect projects by logging into Venafi Web Console and following instructions at Administrator setup.

Create a self-signed CA template

1. From the Certificate Authority Templates node in Venafi Configuration Console, click **Create**, and then select **Self-Signed CA Connector**.
2. Give the new CA template a name. This is the name that will be shown in Aperture when adding a CA template to an environment. Click **Create**. The **Configure New Connector** dialog opens.
3. In the **Settings** tab, enter a **Description** and choose a **Contact** for this template. Select a **Validity Period** for the certificates that will be issued using this template.

4. In the **Key Usage** tab, check the appropriate checkboxes for your purposes. The following key usages and extended key usages are available:

   Only encipherment

   CRL signing

   Certificate signing

   Key agreement

   Data encipherment

   Key encipherment

   Non-repudiation

   Digital signature

   Only decipherment

   Server authentication

   Client authentication

   Document signing

   Time stamping

   Code signing

   > **TIP** Standard code signing certificates have **Digital Signature** and **Code Signing** checked. If you have a special use case, your application might require additional options to be checked

Create Flows

Flows in CodeSign Protect allow you to enforce actions that must take place when using signing keys, when deleting Projects, or when creating, updating, or deleting Environments. There are two types of Flows available, both of which are described below.

Code Signing Flows

Code Signing Flows in Venafi CodeSign Protect define the approvals that must be granted before a signing can take place using a given private key. As such, Code Signing Flows play a critical role in ensuring that private code signing keys are used only in ways that the Code Signing Administrator authorizes.

At their most relaxed, Code Signing Flows can be configured to require no approvals at all. On the other hand, they can also be configured to require multiple levels of approvals. In most companies, a variety of Code Signing Flows are needed to account for the various levels of trust and security demanded by different projects or different phases of projects.

Once created, Code Signing Flows can optionally be assigned to Environment Templates. If assigned to an Environment Template, any Environment that uses that Environment Template is subject to the restrictions set in the Flow. Flows can also be selected directly in Environments themselves.

Code Signing Change Management Flows

Code Signing Change Management Flows allow Code Signing Administrators to use flows to enforce approvals for any of the following:

- To delete a Project
- To delete an Environment from a Project
- To create a new Environment in a Project
- To edit an existing Environment in a Project

The Flows for each of these scenarios can be set individually, giving Code Signing Administrators the ability to manage the different scenarios as their needs dictate. Similarly, the same flow can be used for any number of these scenarios if that's what is needed.

Change Management Flows are set at the global project level, and as such, they apply to all Projects and Environments. The default Change Management Flow requires no approvals. Follow the steps in this section to create a Flow that includes approvals.

Next steps

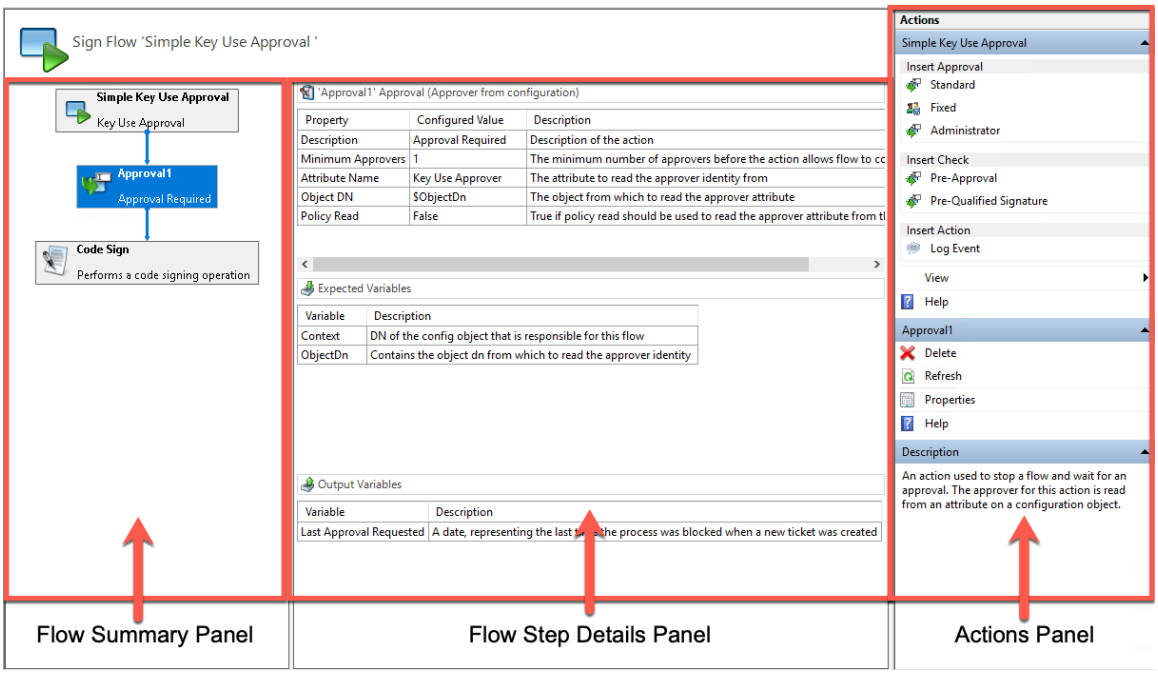
To get started configuring Flow, first become familiar with the Flow user interface. From there, you can configure Code Signing Flows and Change Management Flows. Once the Flows are in place, you can assign them as necessary.

Flow user interface introduction

The Flow configuration screen is divided into three primary panels for both Code Signing Flows and Object Delete Flows. The terms introduced here are used throughout the documentation.

- **Flow Summary Panel**. This panel presents a graphic representation of the steps in the Flow. Clicking on any step opens that step's details in the Flow Step Details Panel.

- **Flow Step Details Panel**. This panel shows the details of the step that is selected in the Flow Summary Panel. This panel is further divided into three sections:
  - **Properties**. Shows the Properties, configured values, and descriptions for the properties of the selected step.
  - **Expected Variables**. Shows the variables that this step expects to receive from the previous step.
  - **Output Variables**. Shows the variables that this step generates upon completion, some of which may be passed to the next step in the Flow.
- **Actions Panel**. Lists the actions that are available to take on the step.



Configure Code Signing Flows

The purpose of Code Signing Flows is to allow Code Signing Administrators to require approvals, checks, and actions before a key can be used to sign. You can open the Code Signing Flows interface by opening the **Custom Flows** node, and then clicking **Add new Code Signing Flow** in the Actions Panel.

The Actions Panel shows the actions that you can add to the flow.

- The **Insert Approval** section includes the options to insert several types of approvals:
  - *Standard* approvals allow you to select either the Project Owner or the Project Key Use Approvers as approvers. These roles are set in the Code Signing Project configurations. See "Add a Standard Approval step" on the next page.
  - *Fixed* approvals are similar to Standard approvals, except that a named approver or group is identified rather than relying on the roles from the Code Signing Project. See "Add a Fixed Approval Step" on page 201.
  - *Administrator* approvals allow you to require approval from Code Signing Administrators and/or Master Admins. See "Add an Administrator Approval step" on page 201.

  When a Key User signs with a key that has a Code Signing Flow that requires approvals, an approval request will be sent to the approvers. Once the approvals are given, the Key User can then re-perform the signing.
- The **Insert Check** section includes the option to add certain pre-signing checks that must be satisfied prior to the signing being performed.
  - *Pre-Approval* provides Code Signing Administrators the ability to approve the use of a code signing key prior to a code signing event. See "Add a Pre-Approval check" on page 202.
  - *Pre-Qualified* Signatures allows you to upload hashes to CodeSign Protect. For Environments that use this Flow, the hash of the code being signed must match a hash that has been uploaded to CodeSign Protect. See "Add a Pre-Qualified Signature check" on page 202.
- The **Insert Action** section allows you to create custom log events to be associated with this Flow.

Code Signing Flows can be configured with any number and any mix actions. The pre-approval action can also be configured to disable any subsequent approval actions in the Flow, dependent upon successful pre-approval.

Set up Code Signing Flows

> **BEST PRACTICE** When an approval ticket is created, the Approvers are written to the ticket, and those Approvers are the only ones who can approve it.
>
> Assigning groups as Approvers (rather than individuals) provides flexibility with who can approve the ticket. Group membership can be changed anytime. So if the Approvers are part of a group, and the group is assigned as the Approver, you then have the ability to manage the effective Approver list independent of the ticket itself.
>
> In general, the more you can do with group assignments, the better.

1. In Venafi Configuration Console, expand the **Code Signing** node.
2. In the **Custom Views** node, click **Add new Code Signing Flow** in the Actions Panel.
3. Give the new Flow a name, and then click **Create**. The name will be used as both the Flow name and as the name of the first step in the Flow. The new Flow is added to the Custom Flows node and the Code Signing Flow configuration screen opens.

Add a Standard Approval step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Standard**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. From the Attribute drop-down, do one of the following:

- Select either **Key Use Approver** or **Owner**, depending on which role you want to assign this approval step to.
- Type in the **Attribute** value manually.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

> **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. If you want to check to see if there is a policy setting for the Attribute value when this step is executed, check **Use policy when reading attributes**. If the Attribute value is set on the policy, it will use what is set on the policy rather than what is set on the object.

g. Click **OK**.

Add a Fixed Approval Step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Fixed**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. Click the **Approvers** drop-down, and then search for the individuals or groups that you want to add as approvers. Use the arrow button to move the approvers from the **Results** box to the **Selected** box. Click **Close**. The approvers are added to the **Approvers** field.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

> **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. Click **OK**.

Add an Administrator Approval step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Administrator**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. From the **Who Approves** drop-down, select which types of administrators can approve.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

> **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. Click **OK**.

Add a Pre-Approval check

a. In the Flow Summary Panel, click the step that should precede the Pre-Approval action.

b. In the Actions Panel, click **Add Pre-Approval action**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. If you want to the flow to disable any subsequent approval actions in this flow, click either **Skip all approval stages**, or select specific stages from the **Skipped Stages** drop-down and add them.

e. Click **OK**.

To apply the pre-approval, either call the AddPreApproval API or use the web user interface.

Add a Pre-Qualified Signature check

a. In the Flow Summary Panel, click the step that should precede the Pre-Qualified Signature check.

b. In the Actions Panel, click **Pre-Qualified Signature**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

To apply pre-qualified signatures, see POST Flow/Actions/CodeSign/PreQualify/Create.

Add a custom log event

a. In the Flow Summary Panel, click the step that should precede the Log Event action.

b. In the Actions Panel, click **Log Event**. Give the log event action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. Complete the log event properties. Note that you can use either the drop-down selections or enter arbitrary text on the **Text 1**, **Text 2**, **Value 1**, **Value 2**, and **Data** fields.

d. Click **OK**.

Edit an approval step

Click the step you want to edit, and from the Actions Panel, click **Properties**.

Delete an approval step

Click any step after the first step, and from the Actions Panel, click **Delete**.

Delete an entire Flow

1. Unassign the Flow from any Environment Templates that use the Flow. Flows that are in use cannot be deleted. See "Edit existing Environment Templates" on page 248.

2. In the Flow Summary Panel, click the first step. In the Actions Panel, click **Delete**.

Next steps

After a Flow is created, it can be added to an Environment Template. In the Environment Template editor, you'll find the **Signing Flow** drop-down menu under the **Settings** tab. From that menu, you can select the Flow. See "Create Environment Templates" on page 207 for more.

Configure Change Management Flows

Code Signing Change Management Flows allow Code Signing Administrators to use flows to enforce approvals for any of the following:

- To delete a Project
- To delete an Environment from a Project
- To create a new Environment in a Project
- To edit an existing Environment in a Project

Enforcing change management provides assurance that critical Projects and Environments and their accompanying keys can't be deleted or changed without approval.

There are three types of approvals available to add to your Change Management Flow.

- *Standard* approvals allow you to select either the Project Owner or the Project Key Use Approvers as approvers. These roles are set in the Project configuration.
- *Fixed* approvals are similar to Standard approvals, except that a named approver or group is identified rather than relying on the roles from the Project.
- *Administrator* approvals allow you to require approval from Code Signing Administrators and/or Master Admins.

In addition, you can add a custom log event action to the flow.

Setting up a Change Management Flow

> **BEST PRACTICE** When an approval ticket is created, the Approvers are written to the ticket, and those Approvers are the only ones who can approve it.
>
> Assigning groups as Approvers (rather than individuals) provides flexibility with who can approve the ticket. Group membership can be changed anytime. So if the Approvers are part of a group, and the group is assigned as the Approver, you then have the ability to manage the effective Approver list independent of the ticket itself.
>
> In general, the more you can do with group assignments, the better.

1. In Venafi Configuration Console, expand the **Code Signing** node.
2. In the **Custom Views** node, click **Add new Change Management Flow** in the Actions Panel.
3. Give the new Flow a name, and then click **Create**. The name will be used as both the Flow name and as the name of the first step in the Flow. The new Flow is added to the Custom Flows node and the Code Signing Flow configuration screen opens.

Add a Standard Approval step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Standard**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. From the Attribute drop-down, do one of the following:

   - Select either **Key Use Approver** or **Owner**, depending on which role you want to assign this approval step to.
   - Type in the **Attribute** value manually.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

   > **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. If you want to check to see if there is a policy setting for the Attribute value when this step is executed, check **Use policy when reading attributes**. If the Attribute value is set on the policy, it will use what is set on the policy rather than what is set on the object.

g. Click **OK**.

Add a Fixed Approval Step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Fixed**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. Click the **Approvers** drop-down, and then search for the individuals or groups that you want to add as approvers. Use the arrow button to move the approvers from the **Results** box to the **Selected** box. Click **Close**. The approvers are added to the **Approvers** field.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

   > **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. Click **OK**.

Add an Administrator Approval step

a. In the Flow Summary Panel, click the step that you want to precede your approval step. For example, if you want to add a step after the "Approval 1" step, then click Approval 1.

b. In the Actions Panel, click **Administrator**. Give the approval action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. (Optional) Enter a **Description** for this step. The description displays as part of the step in the Flow Summary Panel.

d. From the **Who Approves** drop-down, select which types of administrators can approve.

e. Select the **Required number of Approvers** that must approve in order for this approval step to be complete.

> **EXAMPLE** If you selected three approvers, or if you selected a group that has three members, and you want any two of those three to have to approve this request, then select 2.

f. Click **OK**.

Add a custom log event

a. In the Flow Summary Panel, click the step that should precede the Log Event action.

b. In the Actions Panel, click **Log Event**. Give the log event action a name, and then click **Create**. The name you enter will be the name of the step in the Flow Summary Panel.

c. Complete the log event properties. Note that you can use either the drop-down selections or enter arbitrary text on the **Text 1**, **Text 2**, **Value 1**, **Value 2**, and **Data** fields.

d. Click **OK**.

Next steps

After the flow is configured, Code Signing Administrators can now assign it in the global code signing properties. See the "Default Flows" section in "Set global code signing properties" on page 170. This is necessary for the Flows to be invoked.

After an approval Flow is assigned and invoked, the approvers identified in the Flow will be notified, and they will need to either approve or reject the request. See Approving or Rejecting a project deletion request or Approving or rejecting changes to CodeSign Protect Environments, depending on the request type.

Create Environment Templates

Code Signing Environment Templates allow the Code Signing Administrator to suggest or require specific values to be used in CodeSign Protect Project Environments. Each project will include at least one environment.

Add a Single Template

Single templates included just one certificate or key.

Add a Certificate Template

Certificate Authorities are associated with Project Environments, so the options set in the Certificate Environment Template eventually flow into the certificates that get issued.

1. Click **Certificate** from the **Add Single Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   > **DID YOU KNOW?** When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a `- Single` suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as `Development - Single` in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   > **NOTE** A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Certificate Authority	Select which Certificate Authority (CA) Templates will be available to select when creating a Project Environment using this Environment Template. The CA templates must exist in order for them to be selected. For information on creating CA templates, see "Create Certificate Authority (CA) templates" on page 181 . **To add a CA Template** a. Click the **Select Certificate Authority Templates** drop-down and select a CA template to add to this Template. You can also search for a template by typing any part of the template name into the Search box. b. With a CA template highlighted, click **Select**. The certificate path populates in the **Select Certificate Authority Template** box. c. Click **Add**. d. Repeat these steps for any other CA templates you want to add. e. Click **Apply**.
City	The city name that appears as part of the Subject DN of the certificate. This field is also known as the *locale*.
Common Name	The common name (CN) that appears as part of the Subject DN of the certificate.
Country	The two character country code that appears as part of the Subject DN of the certificate. For a list of valid country codes see Country codes.
E-mail	The email address to use as a SAN on the certificate.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add.

Tab	Guidelines
	Any HSM connectors that you have defined will appear in this list.
Keys	Select the encryption algorithms that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.
Organization	The Organization (O) name that appears as part of the Subject DN of the certificate.
Organizational Unit	The Organizational Unit (OU) name that appears as part of the Subject DN of the certificate.
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Certificate Container**: Allows you to specify the location where certificates associated with this environment will be stored. If left blank, the default location specified in the global code signing properties will be used. To view the global default location, click the **Venafi Code Signing** node, and then click **Properties**.

Tab	Guidelines
	Signing Flow: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template.
State	The state (ST) name that appears as part of the Subject DN of the certificate.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add an Apple Template

Certificate Authorities are associated with Project Environments, so the options set in the Certificate Environment Template eventually flow into the certificates that get issued.

1. Click **Apple** from the **Add Single Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Certificate Container**: Allows you to specify the location where certificates associated with this environment will be stored. If left blank, the default location specified in the global code signing properties will be used. To view the global default location, click the **Venafi Code Signing** node, and then click **Properties**. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node.

Tab	Guidelines
	NOTE If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a .NET Template

1. Click **.NET** from the **Add Single Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a `- Single` suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as `Development - Single` in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.
3. Complete the tabs according to the following guidelines:

NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Expiration	The time frame for which a key remains valid before being automatically renewed.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.
Keys	Select the encryption algorithms that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.

Tab	Guidelines
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Key Container**: Allows you to specify the location where keys associated with this environment will be stored. If left blank, the default location specified in the global code signing properties will be used. To view the global default location, click the **Venafi Code Signing** node, and then click **Properties**. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups.

Tab	Guidelines
	Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a GPG Template

1. Click **GPG** from the **Add Single Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a `- Single` suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as `Development - Single` in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Authentication Keys	Encryption algorithms for the GPG authentication keys that you want to make available to Owners to choose from. To make the creation of this key optional, select the **Authentication Key may be optional** checkbox.
E-mail	E-mail address of the person using the GPG key. Together with the Real Name, this becomes part of the user ID (UID). The user ID is used to associate the key with a real person and is used to identify the key when signing.

Tab	Guidelines
Encryption Keys	Encryption algorithms for the GPG encryption keys that you want to make available to Owners to choose from. To make the creation of this key optional, select the **Encryption Key may be optional** checkbox.
Expiration	The time frame for which a key remains valid before being automatically renewed.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.
Real Name	Real name of the person using the GPG key. Together with the E-mail address, this becomes part of the user ID (UID). The user ID is used to associate the key with a real person and is used to identify the key when signing. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider

Tab	Guidelines
	"$IdentityEmail[$Sign.User$]$" Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level.

Tab	Guidelines
	For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178. **Is this template using a Flow that includes approvals? Read more...** If this Template uses a Flow that includes an Approver from Configuration or Fixed Approver action, you need to disable the Command Line instance identifier (which is enabled by default). On the **Request Instance Fields** tab, select the **Use Custom Settings** radio button, then select the instance identifiers you want to use. The recommended defaults are: ◦ **Signing Key Identifier** ◦ **Requesting Machine Name** ◦ **Username of requestor on signing machine**.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Key Container**: Allows you to specify the location where keys associated with this environment will be stored. If left blank, the default location specified in the global code signing properties will be used. To view the global default location, click the **Venafi Code Signing** node, and then click **Properties**. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node.

Tab	Guidelines
	NOTE If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template.
Signing Keys	Select the encryption algorithms for the GPG signing keys that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a Key Pair Template

Certificate Authorities are associated with Project Environments, so the options set in the Certificate Environment Template eventually flow into the certificates that get issued.

1. Click **Key Pair** from the **Add Single Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Expiration	The time frame for which a key remains valid before being automatically renewed.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.
Keys	Select the encryption algorithms that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.

Tab	Guidelines
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Key Container**: Allows you to specify the location where keys associated with this environment will be stored. If left blank, the default location specified in the global code signing properties will be used. To view the global default location, click the **Venafi Code Signing** node, and then click **Properties**. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups.

Tab	Guidelines
	Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a Per-User Template

Per-User templates allow multiple keys or certificates to be associated with a single Environment. This can be useful for things like individual user GPG keys for git signing.

Add a Per-User Certificate Template

Per-user environments allow multiple user-based certificates to be associated with a single environment. In order to help differentiate the certificates that are issued, per-user environments support macros in a number of fields. As such, Code Signing Administrators can use a single per-user environment template to issue unique certificates.

For fields that support macros, the user interface provides suggestions for common macros. You can use the common macros by clicking them. While these macros are suggested, they are not required.

Learn more about using macros

Using suggested macros (available in the user interface)

Following are commonly-used macros, which are suggested in the user interface:

"$Identity[$Sign.User$]$"
Resolves to the username for the key user from the identify provider

"$Identity[$Sign.User$,Given Name]$"
Resolves to given name for the key user from the identity provider

"$Identity[$Sign.User$,Surname]$"
Resolves to surname for the key user from the identity provider

"$IdentityEmail[$Sign.User$]$"
Resolves to surname for the key user from the identity provider

"$Sign.User$"
Resolves to the prefix universal GUID

"$Sign.Project$"
Resolves to the CodeSign Protect Project name, which is set by the Project Owner

"$Sign.Environment$"
Resolves to the CodeSign Protect Environment name, which is set by the Project Owner

"$Sign.EnvironmentType$"
Resolves to the environment type

Using custom macros

You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider:

"$Identity[$Sign.User$,Department]$

Learn more

For additional information on macros, see Macro overview.

1. Click **Certificate** from the **Add Per-User Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a `- Per User` suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as `Development - Per User` in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Certificate Authority	Select which Certificate Authority (CA) Templates will be available to select when creating a Project Environment using this Environment Template. The CA templates must exist in order for them to be selected. For information on creating CA templates, see "Create Certificate Authority (CA) templates" on page 181 . **To add a CA Template** a. Click the **Select Certificate Authority Templates** drop-down and select a CA template to add to this Template. You can also search for a template by typing any part of the template name into the Search box. b. With a CA template highlighted, click **Select**. The certificate path populates in the **Select Certificate Authority Template** box. c. Click **Add**. d. Repeat these steps for any other CA templates you want to add. e. Click **Apply**.
City	The city name that appears as part of the Subject DN of the certificate. This field is also known as the *locale*. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the

Tab	Guidelines
	identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$**

Tab	Guidelines
	Learn more For additional information on macros, see Macro overview.
Common Name	The common name (CN) that appears as part of the Subject DN of the certificate. **NOTE** For per-user Environments, this field requires macros.
Country	The two character country code that appears as part of the Subject DN of the certificate. For a list of valid country codes see Country codes.
E-mail	The email address to use as a SAN on the certificate. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider

Tab	Guidelines
	"$Sign.User$" Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.
Keys	Select the encryption algorithms that you want to make available to Owners to choose from.

Tab	Guidelines
	NOTE The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.
Organization	The Organization (O) name that appears as part of the Subject DN of the certificate. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"**

Tab	Guidelines
	Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Organizational Unit	The Organizational Unit (OU) name that appears as part of the Subject DN of the certificate. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider

Tab	Guidelines
	"$Identity[$Sign.User$,Given Name]$" Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more**

Tab	Guidelines
	For additional information on macros, see Macro overview.
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template. **Container and Naming**: Allows you to specify the path and a name for each user-based certificate. Each certificate must have a unique DN. a. In **Base Certificate Location**, select a location in the Policy tree to use as the base path for all certificates associated with this Environment. b. In **Optional Sub-Folders**, specify any additional sub-folders to append to the Base Certificate Location. This field supports macros, and clicking in the field opens a list of common macros for you to choose from.

Tab	Guidelines
	c. In **Name of the Certificate in the sub-folder**, specify the naming pattern for the certificates. This field supports macros, and clicking in the field opens a list of common macros for you to choose from. The **Calculated Object Name** box shows an example output.
State	The state (ST) name that appears as part of the Subject DN of the certificate. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID

Tab	Guidelines
	"$Sign.Project$" Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a Per-User Apple Template

Per-user environments allow multiple user-based certificates to be associated with a single environment. In order to help differentiate the certificates that are issued, per-user environments support macros in a number of fields. As such, Code Signing Administrators can use a single per-user environment template to issue unique certificates.

For fields that support macros, the user interface provides suggestions for common macros. You can use the common macros by clicking them. While these macros are suggested, they are not required.

Learn more about using macros

Using suggested macros (available in the user interface)

Following are commonly-used macros, which are suggested in the user interface:

"$Identity[$Sign.User$]$"
Resolves to the username for the key user from the identify provider

"$Identity[$Sign.User$,Given Name]$"
Resolves to given name for the key user from the identity provider

"$Identity[$Sign.User$,Surname]$"
Resolves to surname for the key user from the identity provider

"$IdentityEmail[$Sign.User$]$"
Resolves to surname for the key user from the identity provider

"$Sign.User$"
Resolves to the prefix universal GUID

"$Sign.Project$"
Resolves to the CodeSign Protect Project name, which is set by the Project Owner

"$Sign.Environment$"
Resolves to the CodeSign Protect Environment name, which is set by the Project Owner

"$Sign.EnvironmentType$"
Resolves to the environment type

Using custom macros

You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider:

"$Identity[$Sign.User$,Department]$

Learn more

For additional information on macros, see Macro overview.

1. Click **Apple** from the **Add Per-User Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node.

Tab	Guidelines
	NOTE If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template. **Container and Naming**: Allows you to specify the path and a name for each user-based . Each must have a unique DN. a. In **Base Certificate Location**, select a location in the Policy tree to use as the base path for all associated with this Environment. b. In **Optional Sub-Folders**, specify any additional sub-folders to append to the Base Certificate Location. This field supports macros, and clicking in the field opens a list of common macros for you to choose from. c. In **Name of the Certificate in the sub-folder**, specify the naming pattern for the . This field supports macros, and clicking in the field opens a list of common macros for you to choose from. The **Calculated Object Name** box shows an example output.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers.

Tab	Guidelines
	NOTE If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a Per-User GPG Template

Per-user environments allow multiple user-based keys to be associated with a single environment. In order to help differentiate the keys that are issued, per-user environments support macros in a number of fields. As such, Code Signing Administrators can use a single per-user environment template to issue unique keys.

For fields that support macros, the user interface provides suggestions for common macros. You can use the common macros by clicking them. While these macros are suggested, they are not required.

Learn more about using macros

Using suggested macros (available in the user interface)

Following are commonly-used macros, which are suggested in the user interface:

"$Identity[$Sign.User$]$"
Resolves to the username for the key user from the identify provider

"$Identity[$Sign.User$,Given Name]$"
Resolves to given name for the key user from the identity provider

"$Identity[$Sign.User$,Surname]$"
Resolves to surname for the key user from the identity provider

"$IdentityEmail[$Sign.User$]$"
Resolves to surname for the key user from the identity provider

"$Sign.User$"
Resolves to the prefix universal GUID

"$Sign.Project$"
Resolves to the CodeSign Protect Project name, which is set by the Project Owner

"$Sign.Environment$"
Resolves to the CodeSign Protect Environment name, which is set by the Project Owner

"$Sign.EnvironmentType$"
Resolves to the environment type

Using custom macros

You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider:

"$Identity[$Sign.User$,Department]$

Learn more

For additional information on macros, see Macro overview.

1. Click **GPG** from, the **Add Per-User Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   > **DID YOU KNOW?** When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a `- Per User` suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as `Development - Per User` in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   > **NOTE** A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Authentication Keys	Encryption algorithms for the GPG authentication keys that you want to make available to Owners to choose from. To make the creation of this key optional, select the **Authentication Key may be optional** checkbox.
E-mail	E-mail address of the person using the GPG key. Together with the Real Name, this becomes part of the user ID (UID). The user ID is used to associate the key with a real person and is used to identify the key when signing. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID

Tab	Guidelines
	"$Sign.Project$" Resolves to the CodeSign Protect Project name, which is set by the Project Owner **"$Sign.Environment$"** Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Encryption Keys	Encryption algorithms for the GPG encryption keys that you want to make available to Owners to choose from. To make the creation of this key optional, select the **Encryption Key may be optional** checkbox.
Expiration	The time frame for which a key remains valid before being automatically renewed.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.

Tab	Guidelines
Real Name	Real name of the person using the GPG key. Together with the E-mail address, this becomes part of the user ID (UID). The user ID is used to associate the key with a real person and is used to identify the key when signing. For per-user environments, this field supports macros. **Learn more about using macros** **Using suggested macros (available in the user interface)** Following are commonly-used macros, which are suggested in the user interface: **"$Identity[$Sign.User$]$"** Resolves to the username for the key user from the identify provider **"$Identity[$Sign.User$,Given Name]$"** Resolves to given name for the key user from the identity provider **"$Identity[$Sign.User$,Surname]$"** Resolves to surname for the key user from the identity provider **"$IdentityEmail[$Sign.User$]$"** Resolves to surname for the key user from the identity provider **"$Sign.User$"** Resolves to the prefix universal GUID **"$Sign.Project$"** Resolves to the CodeSign Protect Project name, which is set by the Project Owner

Tab	Guidelines
	"$Sign.Environment$" Resolves to the CodeSign Protect Environment name, which is set by the Project Owner **"$Sign.EnvironmentType$"** Resolves to the environment type **Using custom macros** You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider: **"$Identity[$Sign.User$,Department]$** **Learn more** For additional information on macros, see Macro overview.
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178. **Is this template using a Flow that includes approvals? Read more...** If this Template uses a Flow that includes an Approver from Configuration or Fixed Approver action, you need to disable the Command Line instance identifier (which is enabled by default). On the **Request Instance Fields** tab, select the **Use Custom Settings** radio button, then select the instance identifiers you want to use. The recommended defaults are:

Tab	Guidelines
	◦ **Signing Key Identifier** ◦ **Requesting Machine Name** ◦ **Username of requestor on signing machine**.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template. **Container and Naming**: Allows you to specify the path and a name for each user-based key. Each key must have a unique DN. a. In **Base Certificate Location**, select a location in the Policy tree to use as the base path for all keys associated with this Environment. b. In **Optional Sub-Folders**, specify any additional sub-folders to append to the Base Certificate Location. This field supports macros, and clicking in the field opens a list of common macros for you to choose from. c. In **Name of the Certificate in the sub-folder**, specify the naming pattern for the keys. This field supports macros, and clicking in the field opens a list of common macros for you to

Tab	Guidelines
	choose from. The **Calculated Object Name** box shows an example output.
Signing Keys	Select the encryption algorithms for the GPG signing keys that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

Add a Per-User Key Pair Template

Per-user environments allow multiple user-based keys to be associated with a single environment. In order to help differentiate the keys that are issued, per-user environments support macros in a number of fields. As such, Code Signing Administrators can use a single per-user environment template to issue unique keys.

For fields that support macros, the user interface provides suggestions for common macros. You can use the common macros by clicking them. While these macros are suggested, they are not required.

Learn more about using macros

Using suggested macros (available in the user interface)

Following are commonly-used macros, which are suggested in the user interface:

"$Identity[$Sign.User$]$"
Resolves to the username for the key user from the identify provider

"$Identity[$Sign.User$,Given Name]$"
Resolves to given name for the key user from the identity provider

"$Identity[$Sign.User$,Surname]$"
Resolves to surname for the key user from the identity provider

"$IdentityEmail[$Sign.User$]$"
Resolves to surname for the key user from the identity provider

"$Sign.User$"
Resolves to the prefix universal GUID

"$Sign.Project$"
Resolves to the CodeSign Protect Project name, which is set by the Project Owner

"$Sign.Environment$"
Resolves to the CodeSign Protect Environment name, which is set by the Project Owner

"$Sign.EnvironmentType$"
Resolves to the environment type

Using custom macros

You can also use your own macro. For example, the following macro would resolve to the key user's `Department` value from your identify provider:

"$Identity[$Sign.User$,Department]$

Learn more

For additional information on macros, see Macro overview.

1. Click **Key Pair** from the **Add Per-User Template** section of the **Actions** panel.
2. Give the template a name. This name is what Project Owners will see in the web interface when using this Environment Template in code signing projects.

   DID YOU KNOW? When Project Owners select an Environment Template during project creation in the CodeSign Protect web interface, a suffix will automatically be added to the template name you provide here. For example, if you name the template `Development`, it will appear as in the web interface. This is to help Project Owners quickly see whether a project is a single key environment or a per user environment.

3. Complete the tabs according to the following guidelines:

   NOTE A number of the tabs include a **Do not allow users to enter their own values in projects** checkbox. Checking this will restrict the Owner's ability to enter any value other than what is specified in the template.

Tab	Guidelines
Expiration	The time frame for which a key remains valid before being automatically renewed.
Key Storage	Select which Key Storage locations you want to make available. From the drop-down, select an option, and then click **Add**. Repeat for each Key Storage location you want to add. Any HSM connectors that you have defined will appear in this list.
Keys	Select the encryption algorithms that you want to make available to Owners to choose from. **NOTE** The Master Admin sets the system-wide list of available key algorithms. To allow the full list, select the **Use System Defaults** checkbox. To allow only a subset, clear the **Use System Defaults** checkbox, then `Ctrl` + `click` to select the specific algorithms you want to allow. Learn more about supported algorithms.

Tab	Guidelines
Request Instance Fields	Request instance allows you to select which components to use to uniquely identify signing requests. Select whether to **Use Global Settings** or **Use Custom Settings** for this Environment Template. Using custom settings will override the settings that your Code Signing Administrator has set at the global level. For a description of each setting and to learn more about how request instances work work, see "Request Identifier Fields tab" on page 178.
Settings	**Description**: Allows you to specify a custom description for this environment template. The description will appear in the **Actions** panel of the Venafi Configuration Console, and it will also appear in Aperture during project creation. **Signing Flow**: Allows you to specify the Flow associated with this environment. Click the drop-down list, and then search for the Flow you want to add. This list is populated from the **Flows** node within the Code Signing node. **NOTE** If you're changing the Flow on an existing template, this change will be inherited by any existing Environments that use this template. This will clear any approvals in process for Environments using this template. **Container and Naming**: Allows you to specify the path and a name for each user-based . Each must have a unique DN. a. In **Base Certificate Location**, select a location in the Policy tree to use as the base path for all associated with this Environment. b. In **Optional Sub-Folders**, specify any additional sub-folders to append to the Base Certificate Location. This field supports macros, and clicking in the field opens a list of common macros for you to choose from. c. In **Name of the Certificate in the sub-folder**, specify the naming pattern for the . This field supports macros, and

Tab	Guidelines
	clicking in the field opens a list of common macros for you to choose from. The **Calculated Object Name** box shows an example output.
Visibility	Select the users or groups that should be able to see this Environment Template. Leaving this field empty makes this template available to all users. Adding users to this field restricts this template to just those users listed. All users and groups that are currently assigned have visibility. However, you can only *add* users and groups that are part of your identity provider. For example, local users can't add Active Directory users or groups, nor can Active Directory users add local users or groups. Removing users and groups is possible across identity providers. **NOTE** If an end-user does not have visibility to any Environment Templates, they will not be able to create new projects.

After configuring Environment Templates, they are now ready for Owners to use in Code Signing Projects.

Edit existing Environment Templates

From the Environment Templates node in the Venafi Configuration Console, select the Environment Template you want to edit, and then click **Properties** in the Actions Panel. Follow the instructions from the procedure above for guidelines on filling in the template values.

Creating Time Constraints

Code Signing Administrator can create time constraint restrictions that Project Owners can then apply to any CodeSign Protect environment. Time constraints allow the key to be used only at certain times of the day, certain days of the week, certain days of the month, or any combination of these variables.

1. Click the **Time Constraints** node.
2. In the Actions Panel on the right, click **Create Time Constraint**.
3. Provide a name for this time constraint.

The name you enter will be shown to Project Owners when they apply time constraints to environments.

4. In the Time Constraint dialog, do the following:

   NOTE *All* of the criteria that you set in this step must be met in order to use environments where this constraint is applied.

   a. Enter a **Description**. This description will be shown to Project Owners when applying constraints to projects.

   b. (Conditional) Select the **Time of Day** when key use should be allowed.

      - In the **Timezone** drop-down menu, you can either choose a specific timezone or choose Server timezone. Server timezone will use the timezone of the Trust Protection Platform server that performs the signing.
      - In the **From** section, you can specify times of the day when the key is allowed to be used. Leaving *both* fields set to 12:00:00 AM will allow the environment to be used at any time, 24 hours a day.

   c. (Conditional) Select the **Days of the Week** that you want to allow the environment to be used. Leaving them all blank allows every day of the week.

   d. (Conditional) Select the **Days of the Month** that you want to allow the environment to be used. Leaving them all blank allows every day of the month.

5. Click **Apply**, then click **OK**.

This time constraint is now available for Project Owners to apply to their environments.

NOTE Environments can have multiple time constraints applied to them, as long as there are multiple time constraints configured by the Code Signing Administrator. If an environment has multiple time constraints, **only one** of those constraints must be met in order for the environment to be used.

Define allowed signing applications

Venafi CodeSign Protect allows you to restrict what code signing applications are allowed to be used in code signing projects. In addition, you can group applications together into collections. Once the applications and collections are defined, owners of code signing projects can add them to their projects.

NOTE Defining allowed signing applications is an optional restriction. If you don't define any applications, then all signing applications are allowed.

You can identify specific applications using any combination of the following properties:

- **Application Checksum**
- **Authenticode Subject**
- **Authenticode Issuer**
- **Client Filesystem Location**
- **Command Line Regex**

Add a code signing application

1. Open **Signing Applications** in the **Venafi Code Signing** node.
2. In the **Actions** panel, click **Add Code Signing Application**.
3. Enter a name for the application you are adding.

   The name you enter here will appear in the Aperture interface when setting up code signing projects.

   The **Properties** dialog for your new application entry opens.
4. Enter a **Description** for this application.
5. Complete any of the remaining fields to implement restrictions.

   Click the **Load** button to select a signing application on your hard drive. The **Application Checksum**, **Authenticode Subject**, **Authenticode Issuer**, and **Client Filesystem Location** fields will populate with the values from that application. Once populated, you can edit or delete the field values as necessary.

   To use the **Command Line Regex** field, refer to "Using the Command Line Regex field" on the facing page for instructions.

   > **IMPORTANT** Signing applications must meet *all* the properties you specify in order to sign code.
6. Click **OK**.

Add a Collection

1. In the **Actions** panel, click **Add Collection**.
2. Give the collection a name and then click **Create**. This adds the collection as a sub-node under **Signing Applications** and opens that note.
3. In the **Actions** panel, click **Add items to collection**.

4. From the drop-down list, search for the applications you want to add to this collection, and move them from **Results** to **Selected**.

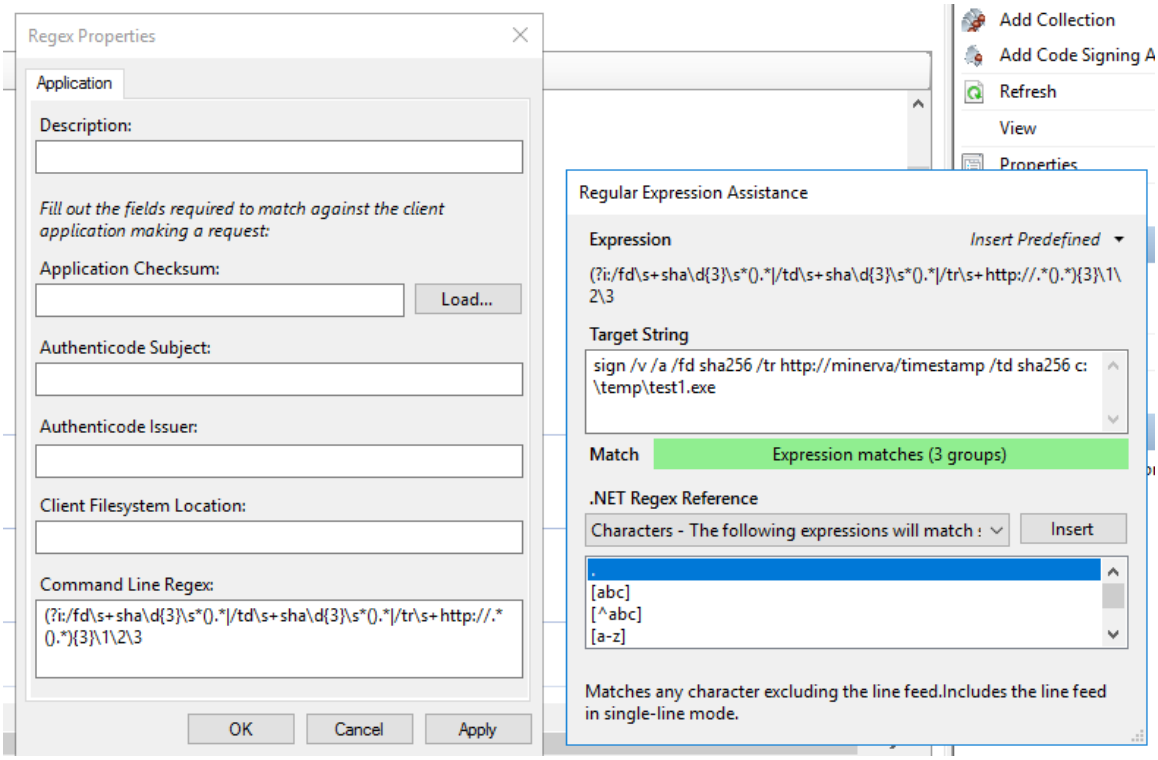
   > **TIP** To see all applications, just enter an asterisk * in the **Search** field.

5. Click **Close**, and then click **Add**.

Using the Command Line Regex field

The Command Line Regex field allows you to enter a regex that the signing command must match in order for signing to occur. Whereas the other options allow you to specify a certain signing application, the regex field allows you to set specific requirements that the signing command itself must meet.

When you click in the Command Line Regex field, the Regular Expression Assistance window opens. While it's not required to use this Window, it can be helpful to ensure that your regex meets your requirements. Using this Window, you can craft your regex, and the test specific signing commands to see if they would be allowed.



Tips on using the Regular Expression Assistance window

- Anything that you enter into the **Command Line Regex** box will be mirrored in the **Expression** space in the assistance window.
- You can use the **.NET Regex Reference** to help craft the regex. Anything you **Insert** from the Reference will populate in the **Command Line Regex** field.
- The **Target String** field allows you to enter a sample signing command. If the string matches the regex, you'll see a green box stating **Expression matches**. Otherwise, the box will be red stating **Expression does not match**.
- The **Insert Predefined** drop-down includes two sample regex expressions that you can use to get started. The two samples are:
  - Signtool with Timestamp `(?i:/fd\s+sha\d{3}\s*().*|/td\s+sha\d{3}\s*().*|/tr\s+http://.*().*){3}\1\2\3`

    This regex enforces the following:
    - The `/fd`, `/td`, and `/tr` switches must all be included, but can be in any order
    - The `/fd` and `/td` switches must be followed by `sha` plus 3 digits (for example `sha256`)
    - The `/tr` switch must be followed by `http://`

    The sample string, `sign /v /a /fd sha25 /tr http://timestamp-server /td sha256 c:\temp\test1.exe`, meets these criteria.
  - Jarsigner with Timestamp `(?i:-tsa\s+http:)`

    This regex enforces the `-tsa` flag followed by `http:`

    The sample string, `jarsigner -verbose /Users/codesign/tosign/test.jar Sample-Development-Environment -tsa http://minerva/timestamp -keystore NONE -storetype PKCS11 -certs -storepass none -providerclass sun.security.pkcs11.SunPKCS11 -providerArg /Users/codesign/venafipkcs11.conf`, meets the criteria.

You can also use this pre-configured online regex tester.

NOTE Limitations:

- There is not any command line detail for applications like PowerShell and excel. The work around for both of these is to use signtool.
- The Command Line Regex option is not available to use with GPG or TKTokenDriver.

Working with signing application collections

For any application collection, you can select it in Venafi Configuration Console and make changes to it. To see the application collections that you have, expand the **Signing Applications** node.

NOTE If you do not have any application collections, the node will not be expandable. For instructions on creating application collections, see "Define allowed signing applications" on page 249.

Click any of the application collections to open that collection. The following actions are available:

- To add items to the collection, click **Add items to collection** from the Actions Panel, and then search for and select the item you want to add.
- To remove items from the collection, click the item you want to remove, and then click **Remove** from the Actions Panel.
- To rename the application collection, click **Rename** from the Actions Panel. The application node name in the left panel becomes editable.

  Renaming an application collection also updates the name in the Projects that use that collection.
- To delete the application collect, click **Delete** from the Actions Panel. If the application collection is used in any Projects, the reference to this application will be removed from the Project.

View credentials

The **Credentials** node is a view-only node that shows the credentials that are currently configured. To view the attributes of a credential, right-click a credential and click **Properties**.

To export a list of credentials, click **Export List** in the Actions Panel.

A single credential can be used in multiple Environment Templates.

To learn more about credentials in Trust Protection Platform, see "Working with system credentials" on page 909 in the *Administration Guide*.

View code signing certificates

The **Certificates** node is a view-only node that shows the currently-issued code signing certificates. Certificates are issued when CodeSign Protect Projects are approved by the Code Signing Administrator.

To view the attributes of a certificate, right-click a certificate and click **Properties**.

To export a list of certificates, click **Export List** in the Actions Panel.

Assign additional Code Signing Administrators

From the **Roles** node in Code Signing, Code Signing Administrators can add and remove other Code Signing Administrators.

To add a new Code Signing Administrator, click **Add Code Signing Administrator** in the Actions Panel, and then select the user that you want to add as an Administrator.

To remove a Code Signing Administrator, click the user you want to remove, and click **Delete** in the Actions Panel.

Venafi CodeSign Protect license not found

The Code Signing Administration node requires a Venafi CodeSign Protect license. If you have not licensed CodeSign Protect, please get in contact with your Venafi sales representative.

If you have your license key and are ready to activate Code Signing, see "Product Licenses" on page 75 for activation instructions.

Events

The Events node is also available as an MMC snap-in called the Venafi Event Viewer.

For detailed information about the Events node, see "Venafi Event Viewer" on page 374.

Statistics

The Statistics node is also available as an MMC snap-in called the Venafi Statistics Viewer.

For detailed information about the Statistics node, see "Venafi Statistics Viewer" on page 384.

Venafi Message Bus

The Venafi Message Bus provides near-instant notifications to other servers in the cluster about significant changes to the database. It is implemented using an MQTT message broker using a publish-subscribe messaging pattern. This allows all servers in the cluster near-instant visibility into the activities and configuration changes of other servers in the cluster.

Messages sent through Message Bus are informative, not authoritative and never contain any confidential data. The message is simply an instruction to other servers that *something* has changed, which allows the other servers to check the database to see *what* was changed, and then take action as needed. This also means that if there are connectivity issues in your network no important data is lost, because the important data isn't the MQTT message itself.

Message Bus is an integral part of the VPlatform service, and a core technology of Venafi Platform. It runs on Venafi servers when the VPlatform service is running. (This service is also known as Venafi Encryption Driver (VED) service.)

Message Bus provides several benefits. For example:

- Servers in the cluster always stay in sync. Configuration changes that used to require users to log out and log back in are now updated to all servers immediately without logging out and back in.
- Permissions are kept in sync. For example, if a user is given rights to a policy folder, those rights are updated across all servers almost instantly.
- Identities and access are constantly updated. When you remove a user from the system, they will lose access right away on all servers, without waiting for their session to refresh. Thus rights and permissions are always kept synchronized.

Configuration Types

Message Bus operates in one of two ways to accommodate all deployment scenarios:

- **Self-Hosted (mesh style).** In this default configuration, each server in the cluster communicates with all other servers in the cluster directly by subscribing to every other server's broker. Every message published from the remote brokers will be passed to the local brokers. This configuration is supported natively by Venafi Platform, and requires no additional configuration as long as the bus port is open to allow communication with all other servers in the cluster. Most customers use this configuration method.

- **Central MQTT Broker (hub-and-spoke style).** In this configuration, all servers in the cluster publish and subscribe to an external MQTTv5 broker, and the broker distributes the messages to all servers in the cluster. This deployment option is provided for customers already using an external MQTTv5 broker and who are required to use that service, or who don't want another broker working on their network. Another reason you might use hub-and-spoke configuration is if your cluster cannot communicate between all servers using the configured port, but the servers can all reach the same external broker. You will need connection information to your central MQTT broker to use this configuration type.

Message Bus is not optional. It is an integral part of Venafi Platform. For new installations of Venafi Platform, Message Bus is configured during the installation steps. For upgrades, the *first* server in the cluster that is upgraded to version 23.3 (or higher) will require you to configure it. Subsequent servers will not require Message Bus configuration on upgrade or installation.

Network Requirements for Message Bus

Message Bus requires correct network configuration. Depending on whether you are using mesh mode or hub-and-spoke mode:

- **Self-Hosted (mesh style).** All servers must be able to communicate with each other over the configured port (default is 8883 for TLS, or port 1883 if you are using an unencrypted bus). Almost all configuration issues are due to incorrect port configuration.
- **Central MQTT Broker (hub-and-spoke style).** Each server must be able to communicate with the central MQTTv5 server over the configured port (default is 8883 for TLS, 1883 if you are using an unencrypted bus.

We suggest you get the network configured correctly before upgrading. Once a server has been upgraded to 23.3 (or higher), you can see if there are any communication issues by looking at the Message Bus node in Venafi Configuration Console where there is a graphical representation of your network which makes it easy to see where any communication issues are detected.

What's Next?

If you are just getting started with Message Bus, see "Modifying Message Bus configuration settings" on page 409.

For details about your Message Bus health and status, see "Working with Message Bus" on page 412.

Modifying Message Bus configuration settings

The information on this page will help you configure Message Bus for your server environment. In its simplest default configuration, Message Bus just works as long as the IANA-assigned port for MQTT (port 1883 for unencrypted, or port 8883 for TLS-encrypted) is open on all Venafi servers. That means you don't necessarily need to configure Message Bus after installation or upgrade.

This topic discusses additional configuration options related to Message Bus you can make in Venafi Configuration Console post installation (or upgrade).

Before you Make modifications to Message Bus configuration

Before modifying the default Message Bus configuration, you need to know the answers to the following questions:

- Do you want to use encrypted MQTT traffic or unencrypted MQTT traffic? (The default is TLS encrypted.)

  While the bus itself doesn't exchange security-sensitive information, the credentials used to authenticate to MQTT might get passed over the wire, which is why we recommend using encrypted communication.

- Do you want to use the default ports? The default port for encrypted MQTT traffic is 8883. The suggested port for unencrypted MQTT traffic is 1883. These are the IANA-assigned ports for MQTT, set by the ISO standard ISO/IEC 20922:2016.[1]

  You'd only want to modify this setting if you have previously assigned the default port for another purpose, or if your network security team asks you to use a different port.

- Do you want to use a self-hosted (mesh) configuration, or do you want to use a central MQTT broker service (hub and spoke) configuration? (The default is self-hosted.)

  Self-hosted (mesh mode) is entirely provided by Venafi Platform. The only reason to use a central MQTT broker is if you are already using one in your organization, and you want to integrate that MQTT broker with Venafi Platform.

- If you are using a central MQTT broker, are you authenticating with a user name and password, or are you using a certificate? If a certificate, do you have the PFX certificate file?

[1]The ISO/IEC 20922:2016 standard is available on ISO.org at https://www.iso.org/standard/69466.html.

To modify Message Bus configuration settings

1. On one of the Venafi servers in your cluster, open Venafi Configuration Console.
2. While on the root node, click the **Configure Message Bus** action in the **Actions panel**.
3. Verify the port number.

   Venafi Platform automatically assigns the default MQTT port for encrypted or unencrypted traffic, depending on your TLS setting. You likely won't need to modify this setting.
4. [Optional] If you require *unencrypted* communication between servers, **Disable TLS**.
5. For Self-Hosted (Mesh) connections between servers:
   a. Click the **Self-Hosted (Mesh)** option, if not already selected.
   b. If you need to change the hostname, click **Override Hostname**.

      #### What is Override Hostname?

      A hostname is one way a computer is uniquely identified on a network. In mesh mode, servers need to be able to communicate with each other, and they identify each server by its hostname.

      The default hostname that Venafi Configuration Console detects for a server might not resolve to the correct address for all servers. An example of this is when using a load balancer, where multiple servers self-identify with the hostname of the load balancer, not the server itself.

      To address this, you can use the **Override Hostname** option, which allows you to enter a fully-qualified domain name (FQDN) that resolves to this server. If you are using TLS, you cannot use an IP address in this field.

      i. Review the Detected name. This is the name that Venafi Configuration Console detected for this host. You can't edit this field.
      ii. Enter a fully-qualified domain name to use to connect to this server in the **Override with** field.
      iii. Click **Save**.
   c. Click **Save**.

d. Ensure all servers in the cluster can communicate to each other using the selected port. In mesh mode all servers need to be able to reach all other servers in the cluster over the specified port. The Message Bus node in VCC will help you identify any communication issues between servers in the cluster.

   That is all that is needed to configure Message Bus in mesh mode. You can skip the next step.

6. For Central MQTT Broker (Hub & Spoke) connections between servers:

   a. In the **Central MQTT Broker** field, enter the URL of the central MQTT broker.

   b. If multiple clusters of Venafi servers are sharing the same central MQTT broker, select a unique **ID** for this cluster. This will ensure the bus correctly interprets which bus messages are intended for this particular server cluster. Other clusters must use a different ID.

      For example, if you have a cluster in your development environment and a different cluster in your production environment sharing the same broker, you would assign different ID values to these clusters so the subscribers can differentiate between clusters.

   c. Make sure the servers can reach the central MQTT broker over the specified port by ensuring the firewall is configured to allow traffic over that port.

      It's easy to see if there are communication issues if you look at the bus overview. If you see all green check marks your ports are configured correctly. If you see red X marks, there is additional information to help you diagnose the issue. See "Working with Message Bus" on page 412 for details on viewing communication status and diagnosing potential issues.

   d. If your broker requires authentication, select an **MQTT Authentication** type.

      i. To use a user name an password:

         i. Click the **Username** option.

         ii. Add your **Username** and **Password**.

      ii. To use a certificate:

         i. Click the **Certificate** option.

         ii. Click the **Load PFX** button.

         iii. Browse to the location of your PFX file and select it.

iv. Enter the Password for your PFX file.

The certificate loads, and you can see its data.

v. If this is the correct certificate, click **Ok**.

e. Click **Validate**to verify communication with the central broker.

Working with Message Bus

The Message Bus node in Venafi Configuration Console shows the status of communications between servers in the cluster. As you hover over the nodes in your cluster, you can see detailed information about the servers and their connectivity to the bus.

Mesh mode

Icon	Status	Description
	Blocked	The server is in the cluster, but cannot communicate with any other servers. For example, the designated port is not open, or the Venafi Platform service might not be running on the server, or the server might be offline.
	Cant Reach All	The server is participating in the bus, but it is not able to reach one or more other servers in the cluster.
✓	Connected	The server is participating in the bus and can communicate with all servers in the cluster.

If you are experiencing connectivity issues, make sure that the firewall settings allow communication over the specified port. In mesh mode, all servers need to be able to reach all other servers in the cluster over the assigned port.

As you hover over servers in the cluster, you will be able to see details about any connectivity issues the servers are encountering. For example, if you hover over a server with a yellow warning symbol, you can see details about which servers it can connect to and which ones it cannot connect to.

Hub-and-Spoke mode

Icon	Status	Description
	Not Connected	The server is not participating on the bus. This may be because the server is offline, or because it is on an older version of Venafi Platform that doesn't support Message Bus, or because the firewall doesn't allow connection to the central broker over the specified port.
✓	Connected	The server is participating in the bus and can communicate with the central MQTT broker.

If you are connected to the server that is not able to communicate with the central MQTT broker, all other servers in the cluster will appear to be disconnected, since this server cannot get information from the broker about the other servers in the bus. If this applies to you, try logging in to another server in the cluster to check its connectivity to help you determine whether the problem is with this server's configuration, or with the central broker.

If you are experiencing connectivity issues, make sure the firewall settings allow communication over the specified port. In central broker mode, each server needs to be able to reach the central MQTT broker over the specified port.

Troubleshooting communication issues

Message Bus is designed to require very little maintenance, so most issues boil down to the following connectivity issues:

- Firewall / Port issues. If the specified ports are not open, the bus nodes won't be able to connect.
- Server status. If the server is powered off, or if the Venafi Platform service isn't running, then the bus clearly can't get updates from the server.

If you need to send a network administrator information to help troubleshoot network connectivity issues, you can click the **Copy health information** link in the **Actions** panel. Connectivity information will be copied to the clipboard so you can send it to the network administrator.

You can quickly see what applications and services are running on each node by clicking the node or click on the server in the graph. **Copy status information** link in the **Actions** panel.

All status information can be copied to the clip board by clicking **Copy Status Information**.

The information from these two links can help you and your network administrators troubleshoot any connectivity issues in the cluster.

Individual engine nodes

If you expand the Message Bus node, the list expands to show all nodes in the cluster. Click on any node to see detailed information about that server.

You see a detailed Engine Status table. It shows services, applications, and service modules running on that server, as well as how long they are have been running and their process identity.

In the Actions panel you can see a description of the selected engine, as well as the measured database latency for that server.

You can specify the hostname used in the mesh by clicking **Set mesh hostname** in the **Actions** panel.

What is Override Hostname?

A hostname is one way a computer is uniquely identified on a network. In mesh mode, servers need to be able to communicate with each other, and they identify each server by its hostname.

The default hostname that Venafi Configuration Console detects for a server might not resolve to the correct address for all servers. An example of this is when using a load balancer, where multiple servers self-identify with the hostname of the load balancer, not the server itself.

To address this, you can use the **Override Hostname** option, which allows you to enter a fully-qualified domain name (FQDN) that resolves to this server. If you are using TLS, you cannot use an IP address in this field.

1. Review the Detected name. This is the name that Venafi Configuration Console detected for this host. You can't edit this field.
2. Enter a fully-qualified domain name to use to connect to this server in the **Override with** field.
3. Click **Save**.

Root Node

On the root node of the Venafi Configuration Console there is a panel that shows the configuration status of the Message Bus. There you can see:

- The operating mode (self-hosted mesh or central MQTT broker)
- The port
- Encryption status (TLS yes/no)
- The hostname of the current server

> **TIP** If you are on the root node and you change the port, you are changing the port for *all servers in the cluster*. If you are in child node and you change the port, you are only changing it for *that specific server*.

Health Check

Message Bus periodically checks to verify that the bus is working as expected. These checks occur five minutes after the VPlatform service starts, and then again every hour. If there is an issue, Venafi Platform will wait fifteen minutes and check again. If there is still an issue, Venafi Platform sends an e-mail notification indicating that there is a health issue with the bus[1].

> **IMPORTANT** If your first installation of Venafi Platform was version 23.1 or older, these e-mail notifications are **not** enabled by default. For information on enabling specific notification rules, see Customizing email notifications. Note that there is one default email notification rule for central configuration, and a different default email notification rule for mesh configuration. Make sure you enable the correct one for your setup.

Tools

The Tools node of Venafi Configuration Console (VCC) contains system tools that help you manage your environment. This node is also available as an MMC snap-in.

As of 25.1, there is only one tool in this node, Logging.

Logging controls all notifications and logging features of Venafi Platform including e-mail templates and e-mail notifications. While most logging and notification features are covered in the topics that follow, you can always refer to the Venafi Log Server Administration Guide (version 25.1) for comprehensive information about the entire logging system.

---

[1]This assumes you have configured SMTP, as no e-mail notifications can be sent by Venafi Platform until SMTP settings have been properly configured.

TIP One frequently used feature of the Tools node is to customize existing log events. To learn more about that, see "Customizing event definitions" on page 425.

Understanding system logging and notifications

With Venafi Trust Protection Platform™, you're not just monitoring and managing your encryption resources–you're also keeping track of those activities and passing along important information about system events as they occur. The platform's log server monitors events and centralizes the logged information. This makes it easier for you to review and assess how your encryption system is performing. Whether you're auditing, troubleshooting, or conducting operational reviews, these logs are your go-to resource.

You can also configure notifications for specific events. By defining notification rules, you can route information about events to a variety of channels like SMTP, SNMP, File, MS SQL, or Sysog, keeping you updated about the events you care about in whatever formats you choose.

Logging overview

The Trust Protection Platform logging system consists of the following components:

- **Events**: Describe an error or status. For example, an event fires when a certificate is about to expire.
- **Venafi log server**: Monitors events, processes logs, and manages sending alert information to specified destinations.
- **Default SQL Channel** : Stores a history of events as a log to a database. These logs can be filtered using a Filter Channel to reduce unwanted or unhelpful event logs.
- **Notification Rules**: Determine which events are forwarded to channels for processing and which events are ignored.
- **Channels**: Manage the delivery of processed log messages in a variety of formats.

The component in Venafi Platform process events, and those events are reviewed by the logging servers. The basic logging of events happens in the default channel. Additionally, based on notification rules, information about events can be passed to channels for delivery to an external system, such as a mail server.

Let's walk through an example:

Imagine Venafi Platform detects a certificate nearing its renewal date. This is an *event*. This information is stored to the *default channel*. Additionally, the log server finds a *notification rule* that matches this event. The notification rule is linked to a specific SMTP *channel*, so the log server passes the information along to the linked SMTP channel.

The SMTP channel is an email notification channel. It uses templates, macros, and message settings to send an email notification to a specified recipient.

If the log server found multiple notification rules for the event, all matching rules would be triggered, and their linked channels would receive the information about the event to process based on their channel settings. So, if there is a matching notification rule tied to a File channel, the event log will be saved to a text file on the corresponding file system.

These are just a couple of examples. Venafi Platform supports several other types of channels for delivering event information based on your organizational needs.

Log server

The Venafi log server serves as the heart of the event logging and processing system, ensuring the events you care about don't go unrecorded.

For a deep dive into managing the Log server, check out "Managing the log server" on page 429.

As a brief overview, the log server:

- **Monitors events**. As Venafi components manage your encryption assets the log server tracks all the events to see if there is a notification rule for each event, and if there is, sends the information to the proper channel for processing.
- **Maintains an audit trail**. Every event gets logged to the default channel, giving you a comprehensive record of all system activities and events. By default, this is an SQL Server channel, and events are stored in either the Venafi Platform database, or another database you configure, however you can use a different channel, like a File channel, as your default if you prefer.
- **Takes actions specified by channels**. When notification rules are triggered by events, the event data is processed by the channel specified in the rule. The log server follows the channel configuration settings to transmit the event log information to the specified destination.

Default channel

Venafi Platform comes configured to store logged event data in its own MS SQL database though a channel called Default MS SQL Channel.

SQL channels store a set of tables and views that automatically capture log information about all system events.

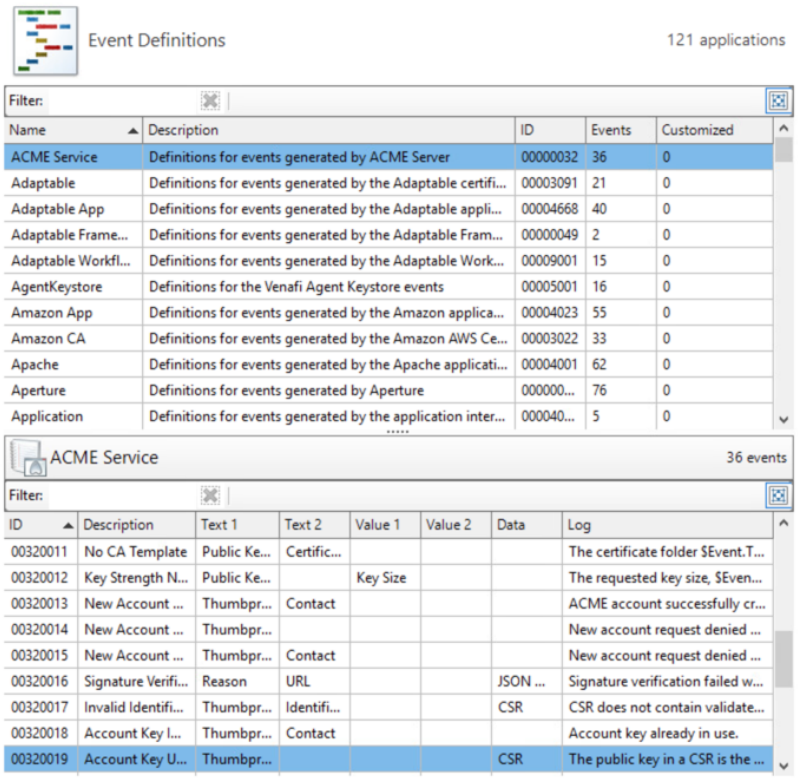
If you need to manage a high volume of events, you can create custom SQL channels to direct logs to other databases. If you need, you can use a Filter channel to ensure you filter out events that aren't interesting to you because of their low severity, or because of some other criteria.

These settings are designed to help you get the right information about the events you care about to the people or systems that need to know about them, and are a critical part of your machine identity management strategy.

For step-by-step instructions on setting up a SQL Server channel, refer to "Creating a SQL Server log channel" on page 448.

Event definitions for server components

All server components have events. The events that the log server tracks are listed in Venafi Configuration Console in the Event Definitions node (**Tools** > **Logging** > **Event Definitions**).



Venafi components are listed in the top table. Click a component to see all the events that the log server tracks for that component. Double-click an event to see how you can customize the description and "translation" of the event. The translation is just a friendly version of the technical log .

As with other tables in VCC (and the MMC snap-in), you can use standard table tools to help you find events in the table. This includes the Filter box, column sorting, and grouping by columns.

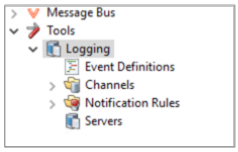
As you make changes, rest assured that your changes will be preserved when you upgrade, and that if you ever want to go back to the default description or translation, it's easy to reset. (The blue arrows on the right will reset the field to its default state.)

Most organizations find the default event definitions meet their operational requirements, so they don't need to customize them, however know that if your needs are different, you can make the needed changes.

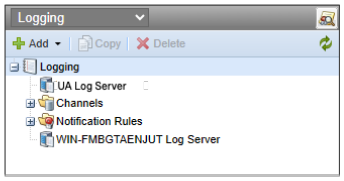
> **NOTE** You must have `Read` permissions to view the objects in the Logging tree, and you must have `Read, Write` if you want to edit them.

Logging tree

If you've used Venafi Platform versions 23.1 or older, you may be familiar with the Logging tree, accessible from the Policy Tree menu. Starting with version 23.3, we recommend you use Venafi Configuration Console (VCC) for modifying logging settings. VCC provides advanced features, and is where you can control all aspects of your log environment, including creating and managing channels, message templates, notification rules and more.



VCC's Tools node



Web Console's Policy Tree

Venafi Configuration Console or the Tools MMC Snap-in?

For consistency, the instructions in this guide always refer to the **Tools** node as being a component in Venafi Configuration Console (VCC). Using VCC requires you to open a session on the Venafi server itself.

The Tools node of VCC is also available as an MMC snap-in from any Windows computer that can make API calls to the Venafi server's SDK endpoint (`[yourserver]/vedsdk`). If you are using the Tools MMC snap-in, when you see instructions to open the Tools node in VCC, you can open the corresponding snap-in collection on your local Windows machine instead, then follow the rest of the instructions as printed.

There is *no difference* in functionality between using VCC or the snap-in collections. Many customers have found that using the various MMC snap-ins make administering their server clusters much more convenient.

To learn how to install and use all the snap-ins, including Tools, see "Install the Venafi MMC Snap-In Collection" on page 363.

Event definitions VCC Node

As discussed in "Event definitions for server components" on page 419, event definitions tell the log server what to pay attention to, and what information to pass along to a notification rule, if the logging server finds a notification rule based on that event.

Channels VCC Node

Channels define the way logs are sent to the correct destinations. The Channels node shows a list of all configured channels. You can edit existing channels and you can create new ones as needed.

The following channels are the possible destinations for a log or notification:

- **SQL Server**. The SQL Server channel allows you to specify a table in a database to store matching log and event notifications. You can write to a table in Venafi's database, or you can use custom connection information to connect to an external database.
- **SMTP**. The SMTP channel lets you send email messages (both plain text and HTML) to specified users. SMTP channels are based on templates, making it very easy to use the same images and style settings for groups of related messages.
- **Adaptable**. Using an Adaptable Channel PowerShell script, you can programmatically send logging events to any destination of your choice, even when it isn't one of the pre-defined channel options in Venafi Platform. For example, if you want to trigger an incident in your ITSM system, you can create a PowerShell script that connects with your ITSM incident management software.
- **File**. Stores notification text in a flat file in the log server's file system or on a network share the log server can access.
- **Filter**. Usually used in combination with the default channel, a filter channel is unique because its target is another channel. The filter channel checks event logs to enure logs you are not interested in aren't allowed to pass along to the destination channel. Other channels typically don't need a filter channel, because the notification rule contains the criteria used to determine if the log should be sent to the target channel
- **SNMP**. The SNMP channel lets you direct traps to an SNMP server. SNMP is a protocol that allows an agent to send an unrequested message to the manager to notify about an important event. Venafi server supports all versions of SNMP.
- **Syslog**. The Syslog channel sends log information to a target host. All variants are supported.

Notification Rules VCC Node

When events happen, the log server reviews the notification rules to determine if the event information should be sent to a channel for distribution. A notification rule is always linked to one or more channels, as notification rules route log messages about events to channels. A notification rule without any channels will not trigger any logging.

Because notification rules can trigger one or more channels, a single notification rule may be sent to multiple channels, which could result in one or more email notifications as well as other logs stored on a file system or database.

Notification rules can also be disabled, in which case they are ignored when the log server processes events.

If you modify the default settings for a notification rule, its changes will be preserved during system upgrades.

Servers VCC Node

The servers node shows you all the servers in your cluster. In large environments, you may have one or more servers dedicated to logging, and this node lets you enable or disable logging on individual servers.

Information about multiple log servers

Venafi Platform supports more than one log server, however you should be aware of the following if you are using multiple log servers:

- All log servers need to use the same default channel. When there are multiple log servers, you can't know which log server will process a notification rule. If you have different default channels on your servers, the logs will be erratic, and finding event logs will be quite difficult.

  If you have multiple log servers with different default channels, you'll see a warning in the **Attention Required** node in VCC.

- If you are using a File channel, you should strongly consider only using a *single* log server. If your file output is saved locally on the Venafi server, you would have incomplete logs that you would need to combine for an accurate, complete log. If your file output is saved on a shared network drive, your

log servers will constantly be competing to write to the file, which will result in errors and incomplete logs.

Log events

Log events are generated by Trust Protection Platform components as well as custom add-ons provided by Venafi, our partners, or customer organizations.

All log events have a standardized set of fields. This allows the log server to store events in a database and query events across all sources.

When an event occurs, the following sequence of events beings.

1. A Trust Protection Platform component serves an event to the Log API.
2. If the event's severity level is `Debug`, and the Debug setting is disabled, it is discarded.
3. The Log API sends the event information to the MSSQL Service Broker Queue for processing.
4. The log server periodically checks the queue.
5. The log server sends the event to the default log channel.
6. The log server applies matching notification rules. This may trigger sending the event information to the corresponding channels.

Event IDs and severity levels

Events have unique event IDs which are 32-bit numbers expressed in hexadecimal. The first four digits define the component. Using these first four characters, you can see how events are grouped by the component that triggers the event, and you can see other events from the same source.

You can see the event ID when you review the event in Logging's Event Definitions node .

All events also have a defined severity level, which helps you assess how critical Venafi considers the event. You can use severity levels in notification rules to help you discover the most important logs.

Severity Name	Critical Rating
Emergency	*Most critical*
Alert	
Critical	
Error	
Warning	
Notice	
Info	
Debug	*Least critical*



Customizing event definitions

You can use the Venafi Configuration Console (or the Logging MMC snapin) to customize existing event definitions.

To customize an existing event definition

1. Open the Venafi Configuration Console (or the Tools MMC snapin), and open the **Tools** node.
2. Click the **Event Definitions** node.
3. In the bottom panel, double click on an **Event**.
4. You can customize both the **Description** and the **Translation**.

Macros are allowed. You can see what content will be provided in the macros when you look at the event definition.

For example, if the content for **Text 2** is "Contact", you could incorporate the corresponding macro, `$Event.Text2$`, like this:

> For additional information, please reach out to $Event.Text2$.

If you incorporated this into an email notification, the resulting paragraph would replace `$Event.Text2$` with the contact's name, and might look like this:

> For additional information, please reach out to Jon Smith.

5. When you're done, click **Apply**.

Resetting to original event definitions

When you change an event definition, it gets marked as "customized" and is protected from changing during upgrade. You can revert an event definition to the default by clicking the Undo arrow next to the event description or the event translation.

> **TIP** If you are having trouble with events after upgrade, it's possible that the default behavior for an event changed, and that is conflicting with a customization you have made. Check to see if you have any customized events by looking on the Events Definitions panel, and reviewing the Customized column. If there are customized events, try resetting them to the default to see if that resolves your issue.

Creating custom logging event definitions

Out of the box, Venafi Platform provides an extensive list of event definitions, however if you find that you need an event definition that is not available you can create your own definitions. For example, if you are a third-party developer, you may want to create logging events tied to the features you are developing.

Event definitions describe the ongoing progress about Venafi or your own add-applications. When an event fires, the Logging application formats the event and it appears on a Policy folder **General** tab and in a MSSQL Logging channel, such as the Default SQL Channel. **When you upgrade to a future version of Trust Protection Platform, any add-on events automatically migrate.**

IMPORTANT We strongly recommend that you avoid making changes directly to the Log schema for events. Instead, you can customize log events that appear in the **Tools > Event Definitions** node of the Venafi Configuration Console (or the Logging MMC snapin). For more information, see "Customizing event definitions" on page 425.

When adding your own logging events:

- Make sure each add-on has its own unique Group ID. Use the reserved decimal range of `0200`-`0299`.
- *EventID*s must be unique. For example, you can use Group ID `0200` and assign EventIDs from `0200000` through `0200FFFF`.
- Comma separate each field and leave unnecessary fields blank.
- Use macros to allow the Logging application to add dynamic information. For more information, see Using the $Event.Formatter$ macro. For example:

  ```
  02001FAF,Custom App - Certificate Expiration Processing,,,,,,,,,,"Service module for the engine $CN [$EHvent.Component$]$ is examining certificates for expiration."
  ```

  When this event triggers, the Log server records the following event:

  ```
  127.0.0.1, 17/08/2009 22:17:42: Service module for the engine Jupiter is examining certificates for expiration.
  ```

2

Managing the log server

The Venafi Platform log server manages the flow of information to the default channel, interprets notification rules, and utilizes channels to deliver targeted log messages based on those rules. It reviews defined events, then logs all events to the default log channel to ensure there is a complete audit trail of all system operations and events. Once an event is logged to the default channel, the log server checks notification rules to see if any rules match. If there is a matching notification rule, the log server forwards the log data to the appropriate channels, which deliver the log to the defined service, location, or person.

The Servers node shows the log servers in the cluster, and is where you can specify the default log channel.

As a safeguard, whenever you make configuration changes to the default log channel, you need to restart the log server service. All other channel changes will refresh after configuration changes, and do not require a service restart.

This chapter contains the following topics:

Reviewing log events in VCC

You can use the Venafi Configuration Console to review events in the following ways:

- View all events or create a custom view that filters just the events you want.
- Create custom views of events you want
- Save events to a .CSV file for reference
- Import earlier-saved .CSV event files
- View statistics about events
- See an overview of events logged over recent time periods (one hour, one day, one week). This is a useful feature that gives you a quick overview of your system's event history without needing to read individual logs.

To review log events in VCC

1. In Venafi Configuration Console (VCC), open the **Events** node.

   > **TIP** If you are using the MMC snap-ins, be aware that Events is a separate snap-in from Tools, and has to be loaded separately.

2. The following table shows some of the things you can do to review recent events.

Action	Description
Report events by time period, and occurrences	Review the Log Summary table. ◦ **Event Type** describes an event severity. If there are any logged events during the last week for that event type, you see a plus icon. Click that to see the events in that categorty. ◦ **Event ID** provides the event message. ◦ **Source** identifies the component that fired the event. ◦ **Last hour**, **24 hours**, **7 days** show the cumulative number of occurrences for a time period.
Sort, group, and Drill Down	Click on a column header to sort by that column.

Action	Description
	Right-click on a column header to see grouping options. You can group by this column, or you can Show GroupBox, which allows you to create advanced grouping rules that can help you locate events quickly. Right-click on cell data to use the Drill Down feature. The Drill Down options depend on the type of information in the cell. For example, clicking on a source value in the All Events list lets you see all events from that source, or from the same component, or during a specified time frame. Clicking on a certificate renewal event lets you see all the other events that were tied to that certificate's renewal action (like workflow approvals, and so on). As you use Drill Down you'll see temporary views based on your drill-down criteria appear in the Events node. (These are session-specific and are removed when you close VCC or the snap-in.)
Show all events	Click **All Events**. The same sorting, grouping, and Drill Down features are available for All Events.
Create a custom View	a. Right click **Custom Views** and select **Create Custom View**. Filter, and then click **OK**. Filters: • **Event level** describes the event severity. • **Event sources** match an Event Definition in the Policy Tree Logging tree. • **Limit to** shows the number of the newest events. b. On the **Save Filter to Custom View** screen, type a **Name** and **Description**, and then select or create a VCC folder for the log. c. Click **OK**.

Action	Description
Create custom view filters	a. Click **Custom Views** and the view name. b. (Optional) In the **Actions** pane, click **Filter Custom View**, select options as appropriate, and then click **OK**.
Export a custom CSV log	a. Open the custom view and in the **Actions** pane, click **Save Event Log as**. b. Specify a path, and then click **Save**.
Import a custom CSV log	a. Click a custom view and in the **Actions** pane, click **Open Saved Log.** b. Specify a path, and then click **Open**.

For more information about using the Venafi Event Viewer, see "Venafi Event Viewer" on page 374.

Manually stopping and starting the log server service

The Venafi log server service manages event logging and notifications. If you need to stop, start, or restart the log server service, use the following instructions.

If the log service is running, and you want to restart it

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel.
3. Click the **Restart** action.

   The service will stop, then restart. The process is complete when you see the service change back to **Running**.

To manually stop the log server service

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel.
3. Click the **Stop** action.

   This sets the status to **Stopped**.

To manually start the log server service

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel
3. Click the **Start** action in the right panel.

   This sets the status to **Running**.

Configuring the log server

The log server represents the service that manages all logging and notification functions for a particular server. The log server is automatically created when you install Trust Protection Platform on a server and can be seen in Venafi Configuration Console (VCC) under **Tools** > **Logging** > **Servers**. Each server in the cluster has a separate server entry.

> **IMPORTANT** Whenever you make configuration changes to the default log channel, the Logging service requires a restart. All other channel changes will refresh after configuration changes without requiring a restart of the Logging service.

To configure the Log Server using VCC

1. In Venafi Configuration Console (VCC), open the **Tools** > **Logging** > **Servers** node.
2. From the list of log servers, click the specific server you want to configure.
3. Click **Properties** in the **Actions** panel.
4. Make the configuration changes.

   Refer to the table below for the options.
5. Click **OK** or **Apply**.

Property	Description
Description	A friendly description for the server.[1]
Default Channel	The Venafi log server records all events to a log table in the Trust Protection Platform database. If you want to see log events onscreen, you must use a database channel as your default log channel.[2] **IMPORTANT** You must ensure the database server that stores the channel data does not run out of disk space. If the server runs out of disk space, the log server cannot operate. The space you need for your log store depends on a number of factors that include, but are not limited to, how many events per second you are storing and how long you want to keep the data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring. **WARNING!** If you are using your Venafi server as your logging server, if your server runs out of disk space, the *entire set* of Venafi services on that server will stop working.
Server Disabled	Controls whether this server will process log events or not.

You can see the server's details in the bottom panel including the channels and notification rules that this log server processes.

Controlling the size of the log

Trust Protection Platform logs event data into a centralized database so you can review and evaluate your system activity. The logged information is helpful for auditing, troubleshooting, and operational reviews.

Typically, the channel that is used is the Default SQL Channel. Its job is to log all events.[3] Over time, the number of log entries can accumulate, taking up disk space and making the data more difficult to search and use. Minimizing the total number of logged events in the database improves the usability of the data and minimizes disk space usage.

---

[1] On the Actions panel of the main Log Servers page you have an option to rename the log server to change the server's name in the list.
[2] Technically you can also use a filter channel as your default log channel as long as it points to an SQL database channel.
[3] In its default configuration, an SQL Server channel logs all system events. However, you can use a Filter channel to discard some events so your logs are more relevant and take up less space.

IMPORTANT If you do not want to delete logged events at all, you can disable log expiration altogether. However, if your log file is not managed correctly, it can grow large enough to use up all remaining disk space and significantly impact server performance.

You can specify how many days each log entry is kept before it is deleted automatically. When a logged event exceeds the number of days you specify, the log entry is deleted permanently.

NOTE The default setting for log event deletion is 90 days. You can set any value between 0 and 3650. A setting of 0—or if you leave the value blank—disables log expiration.

To configure log event expiration in VCC

1. In Venafi Configuration Console, navigate to **Tools** > **Logging** > **Channels**.
2. Click **Default SQL Channel** in the center panel.
3. Click **Properties** in the Actions panel.
4. In the **Automatically delete records older than** field, set the number of days to maintain logs for this channel.

   The default number of days is 90.
5. To disable automatic deletion of logs, uncheck the **Automatically delete records ...** option.
6. Click **OK**.

TIP Log expiration can also be set during the initial installation of Venafi Platform, and is one of the settings in the XML answer file you can use to provide initial configuration information for new servers.

Setting up SMTP settings for outbound email connections

Venafi Platform has powerful logging capabilities, with a variety of methods of delivery. After database logging, the most popular form of notifications is via email.

Venafi Platform will *not* be able to send email notifications for log channels or for the reporting service until you configure the outbound SMTP server settings, as described below.

The SMTP server settings you want to use may be the same for both log channels and the reporting service, however you need to set up both if you are using both features. Keeping the configurations separate allows you to use different email settings for the different purposes.

Configuring the SMTP Default Connectors for Log Channels and Reporting in VCC

1. In Venafi Configuration Console, open the **Connectors** node.
2. In the SMTP Default Connectors section, click the connector you want to configure.
    - **Log Channels**. This connector controls the SMTP email configuration for all SMTP Log channels. For more information, see "Setting up notification channels" on page 439
    - **Reporting**. This connector controls the SMTP email configuration for all Reporting service modules.
3. Click **Properties**.
4. If prompted, log in to Venafi Platform using an account with system administrator permissions.

5. Enter the SMTP Server information as outlined in the table below.

Field	Description
Host	Enter the SMTP host name or IP address. For example: `smtp.example.com` or `127.0.0.1`.
Port	Enter the port to use for the SMTP connection. The default port for SMTP connection is 25, which does *not* encrypt the connection. To use Secure TLS communication, you cannot use port 25. Here are the three standard SMTP ports: ◦ Port 25. (Default) This is a non-secure default SMTP port. ◦ Port 465. This port securely sends email via SMTP by SSL/TLS. ◦ Port 587. This is the successor port of port 465 and is often seen as the default transmission channel for secure SMTP connections. **About secure SMTP connections** Venafi uses SMTP Authentication for outbound email. We are investigating support for OAuth2, but the currently-implemented OAuth2 flows are created for client applications where the user can be periodically prompted for credentials (or MFA) to obtain a new grant. As a server application, Venafi requires an unattended authentication method. We strongly recommend you configure your SMTP to use Secure TLS communication on a supported port. The Microsoft Exchange team's solution for continued support is using High Volume Email (HVE) for Microsoft 365, Azure Communication Services for Email, or an Exchange Server on-premises in a hybrid configuration. For instructions on how to onboard to High Volume Email for Microsoft 365, see instructions from Microsoft at https://learn.microsoft.com/en-us/Exchange/mail-flow-best-practices/high-volume-mails-m365. This solution uses port 587 and authenticates to Office 365 using a HVE account username and password.
Sender E-mail	This is the e-mail address the recipient will see in the "From" field of their email message.
Use Secure	This setting enables the email client and server to exchange messages using

Field	Description
TLS communication	the Transport Layer Security (TLS) protocol, which encrypts the data and verifies the identity of and integrity of the parties involved.
Log event for each delivered message	When checked, Venafi Configuration Console will log an event for every email message it sends. This feature is useful to meet some organization's auditing requirements.
Lock settings [...]	When checked, individual SMTP channels or Reporting modules will not be able to override these settings. This is analogous to locking the policy setting.
Authenticate to SMTP Server	This setting requires the email client to provide a valid user name and password to the SMTP server before it can send or receive email messages. When selected, the following two fields become available.
Username	The username used to authenticate the SMTP connection to the email host.
Password	The password used to authenticate the SMTP connection to the email host.
Send Test E-mail	Click to test the connection to ensure Venafi Platform can send messages using these settings.

6. Click **OK**.

IMPORTANT Until SMTP outbound server settings are configured for the first time, SMTP channels are disabled. Do not attempt to send any logs to SMTP channels until you configure SMTP outbound server settings as described above.

The first time you configure an SMTP connection, the built-in SMTP channels automatically become enabled.

3

Setting up notification channels

Channels provide the targets for where and how event logs are stored or transmitted to an external service. Channels are configured and managed in Venafi Configuration Console's **Tools** > **Logging** node.

Channels store the information the Venafi log server needs to deliver the log to the desired target. For example, MS SQL channel objects include the information needed to store messages in a database. SMTP channel objects include the information needed to send email messages with logged event information.

> **NOTE** Venafi Platform channels support both IPv4 and IPv6 connections.

This chapter contains the following topics:

Chapter 11: SQL Server channel requirements 290

Chapter 12: SQL Server channel configuration 291

Chapter 13: Updating the SQL Server channel object 294

Chapter 14: Creating a SQL Server log channel 294

Chapter 15: SMTP channel factory template upgrade considerations 297

Chapter 16: SMTP outbound server configuration 297

Chapter 17: Email templates 298

- Email Templates in VCC 298
- Customization and Upgrades 299

Flexibility in Configuration ... 299

Chapter 18: Managing logos and images used in email templates ... 299

Chapter 19: About SMTP templates for email notifications ... 302

Where to Find Templates ... 302

Customizing Templates ... 302

Setting the Default Template ... 302

Preservation During Upgrades ... 303

Resetting to Default Configuration ... 303

Chapter 20: Editing SMTP message templates ... 303

Using the Template Editor ... 304

Working with macros, images, and variables ... 304

Chapter 21: Built-in SMTP channels ... 306

SMTP channel properties ... 307

ChapterEditing SMTP channel message contents for email notifications 22: ... 311

Specify a template ... 311

Preview the message ... 311

Define variable values ... 311

Chapter 23: Message delivery failures ... 312

Chapter 24: Adaptable Log Channel prerequisites ... 313

What's next? 314

Chapter 25: About the Adaptable Log Channel PowerShell script 314

ChapterExample: creating a ServiceNow incident for expiring certificates
26: 317

Chapter 27: Configuring the Adaptable Log Channel object 318

ChapterProtecting against unapproved changes to Adaptable Log Channel
28: scripts 321

Chapter 29: PowerShell script reference for Adaptable Log Channel 322

About debug logging 323

Chapter 30: About hash tables 324

Chapter 31: Perform-Action function 324

Chapter 32: File channel requirements 329

Chapter 33: File channel configuration 329

Chapter 34: Filter channel configuration 333

What happens if I select items for both Events and Severity? 334

SNMP Versions and Compatibility 334

Management Information Base (MIB) 335

Customizing the MIB 335

Chapter 35: SNMP channel requirements 335

Chapter 36: SNMP Channel object configuration 336

Chapter 37: Customizing the Management Information Base 339

About the CEF format 341
About the JSON format 341
About the BSD format 342
About TLS 342
Chapter 38: Syslog channel prerequisites 342
Chapter 39: To configure a syslog channel object 343

About configuring the Channels folder

The Channels folder contains objects that manage communication between Trust Protection Platform and other external services and that are receive event logs and messages. The Channels folder stores:

- The Default SQL Channel, which is where all logs are stored by default.
- A folder of Built-in channels.
- Any additional folders and channels you create.

IMPORTANT E-mail notifications can only be sent if the **Log Channels** SMTP Default Connector is set up correctly. This is configured on the **Connectors** node in VCC. For detailed steps, see "Setting up SMTP settings for outbound email connections" on page 435.

Creating Channel objects

Trust Protection Platform is designed so you can create multiple channel instances for any given channel type. This means you can create multiple channel configurations to handle different functions or events. For instance, you can configure the Venafi Log server to use one MS SQL Channel object as the Default SQL Channel and another MS SQL Channel as a specialized log store for specific types of events.

You can also define multiple SMTP channel objects to send notifications to different recipients such as the contact for each application that consumes a given certificate, the certificate contact, the system administrator, and a certificate approver. Every SMTP channel object supports both plain text and HTML messages.

> **NOTE** To view examples of channel object configurations, review the default channel objects that are provided in the **Channels** > **Built-In** node. You can use the default channels as-is, you can modify the default channels, or you can reference their configurations as a guide to help you create your own channel objects.
>
> If you modify a default channel, you can revert it to it's factory settings at any time by clicking on the channel, then clicking the **Revert** action.

To create a channel object in VCC

1. In Venafi Configuration Console (VCC), browse to the **Tools** > **Logging** > **Channels** node.
2. In the **Actions** panel, click the type of channel you want to create.
    - **SQL Server**: Log events to a Microsoft SQL Server database. For more information, see "SQL Server channel" on page 443.
    - **SMTP** Forward logged events to specified a specified email destination. For more information, see "SMTP channel" on page 450.
    - **Adaptable**: Log events to a custom channel. For more information, see Using Venafi's Adaptable Log Channel.
    - **File**: Log untranslated or translated events to a human-readable log file. For more information, see "File channel" on page 481.
    - **Filter:** Log events based on event type or severity to reduce the number of events logged to a database. For more information, see "Filter channel" on page 486.
    - **SNMP**: Forward logged events to an Simple Network Management (SNMP) system. For more information, see "SNMP Versions and Compatibility" on page 488.
    - **Syslog**: Forward logged events to a syslog server. For more information, see "About the CEF format" on page 495.
3. Complete the channel configuration, then click **OK**.

SQL Server channel

The SQL Server channel allows the Venafi log server to record events to a Microsoft SQL Server database. To store events, you can use the Trust Protection Platform database that you set up during installation or create a custom database.

IMPORTANT Venafi highly recommends stopping all Trust Protection Platform services prior to any scheduled database maintenance. Neglecting to so may produce unexpected behavior because Trust Protection Platform is dependent upon the database for the majority of its configuration and certificate data. Trust Protection Platform has been designed to handle brief loss of database connectivity due to network issues or similar anomalies but that should not be relied upon for extended database outages, especially those which are planned.

SQL Server channel requirements

Trust Protection Platform logs events to the location that is defined in the default channel. At installation time, the events log to the Trust Protection Platform database. However, if there are large volumes of events, you may want to consider creating a separate database and corresponding custom SQL Server channel just for processing log events.

As a general baseline, Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring. The space you need for your database depends on a number of factors. These include, but are not limited to, how many events per second you are storing and how long you want to keep the data.

IMPORTANT You must ensure the database server that stores the channel data does not run out of disk space. If the server runs out of disk space, the log server cannot operate.

The space you need for your log store depends on a number of factors that include, but are not limited to, how many events per second you are storing and how long you want to keep the data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.

WARNING! If you are using your Venafi server as your logging server, if your server runs out of disk space, the *entire set* of Venafi services on that server will stop working.

When using a separate MS SQL database, please refer to the Supported Databases section in the general System Requirements, as the specifications are the same.

For more information about Trust Protection Platform system requirements, see System requirements for Venafi components in the *Trust Protection Platform Installation Guide*.

SQL Server channel configuration

The SQL server channel stores information that the system needs to write events to an SQL Server database. During installation, Trust Protection Platform uses the database connection information to create the Default SQL Channel. This is the datastore where the Venafi log server logs all events.

For details on the SQL Server channel configuration, see "Updating the SQL Server channel object" on page 448.

Field	DSN Type	Description
Table	System, Custom	Specify which existing table in the connected database to use for the logs sent through this connector. This table must already exist.
Automatically delete...	System, Custom	Continually prunes log entries from the target database for logs older than the specified interval. We recommend you leave this setting enabled unless operational requirements (like legal data retention requirements) tell you otherwise. **IMPORTANT** It is very important that you properly manage log file size. If the server runs out of disk space, the log server cannot operate. If the database is on the same server as Venafi Platform and the server runs out of disk space, you will likely have a service outage. The size of your log store depends on a number of factors that include the number of generated events per second and the retention period for data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.
DSN	System, Custom	You can choose one of two database options: ■ Use system DSN. Use the same database that Venafi Platform is using.

Field	DSN Type	Description
		■ Custom Connection Data. Use a different database to store logs sent through this channel. **NOTE** The rest of the fields below are *only* displayed if you choose the Custom Connection Data option.
Username	Custom	The account name that the Log server uses to authenticate with the custom database. This account must have `db_datawriter` and `db_datareader` in the log store database. Requires additional grants. For more information, see "Creating a SQL Server log channel" on page 448.
Password	Custom	The password that the Log server uses to authenticate with the custom database.
Host	Custom	The IP address or hostname of the custom Microsoft SQL database server. Trust Protection Platform supports both IPv4 and IPv6 connections to MS SQL database servers. If a hostname is specified, only the first resolved address associated with that name is used.
Port	Custom	The port where the Log server connects to the custom database. For example 1433.
Database	Custom	The name of the custom database where the Log server writes events. This database must already exist. The SQL Server channel driver does not create the database.

Field	DSN Type	Description
Encrypt all database communications	Custom	Enabling this option encrypts all communications between the Trust Protection Platform server and the custom back end database. If this option is not selected, the credentials are still protected but all other communications between the server and the database might not be protected. Recommendation: Enable To learn how to enable SSL encryption for an instance of SQL server by using Microsoft Management Console, visit: https://support.microsoft.com/en-us/help/316898/how-to-enable-ssl-encryption-for-an-instance-of-sql-server-by-using-mi.
Windows Authentication	Custom	Windows Authentication will be used for the database connection. If you select this option, Log server authenticates to the database using a Windows user account and password instead of database credentials. Be sure to verify the following configurations: ■ All Log servers must use Windows Authentication credentials. ■ All Trust Protection Platform servers provide Windows Authentication for Policy Tree. ■ The Windows Authentication credentials have access to the database. When you select this option, the **Username** and **Password** fields, above, are disabled.
Enable "AlwaysOn Availability Groups" support	Custom	The Always On Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. For more information, see Always On Availability Groups (SQL Server).

Updating the SQL Server channel object

During installation, Trust Protection Platform automatically creates a database table and configures the default SQL Channel object to store log events in the table. The default SQL Channel object controls the location where the Log server stores event logs.

The default SQL Channel only requires configuration if you are using a separate database to store log events. A separate database for event logging requires you to create a custom SQL channel, and then change the default SQL channel object.

To update the default SQL channel object

1. Log in to Venafi Configuration Console (VCC) and browse to the **Tools** > **Logging** > **Channels** node.
2. Click **Default SQL Channel**, then click **Properties**.
3. Configure the other settings as described in "SQL Server channel configuration" on page 445.
4. Click **Save**.
5. Restart the Log service.

Creating a SQL Server log channel

When you're dealing with a high volume of log events, a custom SQL log channel can be helpful. By setting one up in the Venafi Configuration Console, you can direct events to an additional database you've created. This way, depending on your notification and policy settings, Venafi Platform will log events to either its own database or your new custom database.

Initial database setup

- **Create Database**: Open SQL Server Management Studio and create a new database.
- **Server Requirements**: If you're using a separate SQL Server for your custom log database, make sure it meets Venafi's database server requirements. For details, see System requirements for Venafi components.
- **High-Availability** (Optional): You can configure the SQL Server for high availability using Microsoft's Always On Availability Groups. For more information, see Always On Availability Groups (SQL Server).
- **Database Naming**: Database names must follow standard Venafi requirements.

  The database name cannot contain any of the following characters:

  ```
  [](){}\"',$%*?
  ```

Script Execution

1. Open script.

   Navigate to *[Venafi installation folder]\Database Scripts\MSSQL\Updates\Optional\mssql_log_structure_SP.sql*.

2. Run script.

   Run *mssql_log_structure_SP.sql* against the new database. This will generate additional stored procedures, tables, and types.

3. Create Log Channel.

   On the new database, run *DAL_LOG_SP_CREATE_LOG_CHANNEL 'table prefix'*. For example, *exec dbo.DAL_LOG_SP_CREATE_LOG_CHANNEL 'Log3'*.

4. Account Permissions. (Optional)

   If you're using an account other than `sa`, run the following set of grants listed below:

   - Open *[Venafi installation folder]\Database Scripts\MSSQL\Updates\Optional\mssql_log_grant.sql*.
   - Follow the instructions in the `mssql_log_grant.sql` file to grant permissions to an operational database account.

Configuration in Venafi Configuration Console (VCC)

1. Create SQL Server channel.

   In Venafi Configuration Console, expand the **Tools** > **Logging** > **Channels** nodes, then click **SQL Server** in the Actions panel, and give the new channel a name.

2. Configure the channel.
   - Specify the database **table** to use to store the logs.
   - Decide if you want to automatically delete records after a specified number of days.

     We strongly recommend you enable this option unless you have a specific operational requirement to maintain logs. If you don't purge log files regularly, your database can get very large, and if you log enough events, can even run out of storage space.
   - Choose **Custom Connection Data**.
   - Enter the database connection information.

Final steps

1. Create notification rules.

   You'll need to create the notification rules that will be stored to this database, and you will need to point them to your new custom SQL Server channel. For more information see "Working with notification rules" on page 501.

2. Restart log server.

   In VCC, go to the **Product** node, and click the **Logging** Windows service. In the **Actions** panel, click **Restart**.

SMTP channel

The SMTP channel delivers logging data to email through an SMTP server.

To send notifications using an SMTP channel, administrators can do any of the following:

- Use the built-in SMTP channels. These channels already have notification rules associated with them and will start working as soon as an outgoing SMTP server is configured.
- Edit the built-in SMTP channels. You can edit them directly, or duplicate them and modify the copies.

- Create new SMTP channels. You can configure notification rules to point to new SMTP channels you create. Once your new SMTP channels have been configured, see "Working with notification rules" on page 501.

SMTP channel factory template upgrade considerations

Venafi Platform offers a range of pre-configured SMTP channels for a wide variety of events. Feel free to use these channels as they are, tweak them to better fit your needs, or duplicate them to create customized channels.

Starting with Venafi Platform version 25.1, any changes you make to these default channels will stick around, even after system upgrades. Plus, you can always revert to the factory settings of any built-in channel whenever you like.

> **EXAMPLE** Consider the following scenario:
>
> Let's say you installed Venafi Platform version 25.1 and customized a default email channel to align with your company's requirements. When you later upgrade to version 24.1, your customizations will be preserved.
>
> So, what if Venafi updates that channel in a future release, like 25.1? No worries—your changes will still be there after the upgrade. If you ever want to go back to the factory settings, simply choose "Reset customization" from the VCC Actions menu. This will revert the channel to the most recent factory version—in this example, version 25.1.

SMTP outbound server configuration

SMTP channels need to communicate with an external SMTP server so logs can be delivered as email messages. The outbound SMTP server configuration is found in VCC in the **Connections** node.

For specific steps on adding SMTP server connection information so the SMTP channels can delver notifications, see "Setting up SMTP settings for outbound email connections" on page 435.

Until the outbound SMTP server settings are configured for the first time, SMTP channels are disabled. Venafi Platform automatically performs a one-time process to enable the SMTP channels as soon as the outbound SMTP server settings are first set up.

Email templates

Venafi Platform's SMTP channels are designed to send multi-part email messages, which include both HTML-formatted and plain-text content, to designated recipients.

Here's a quick refresher on how emails are generated in Venafi Platform

The log server watches for events that match notification rules. When an event matches a notification rule, the notification rule passes log information to a channel; in the case of email messages, it is an SMTP channel. The SMTP channel applies an email template, resolves the macros, inserts the log information, and sends the email to the desired recipient.

Email Templates in VCC

In Venafi Configuration Console (VCC), you'll find email templates that come with common formatting elements like logos, CSS styles, and message footers. These templates feature placeholders where the SMTP channel fills in the actual log content.

The beauty of these templates is that they centralize common elements. If you need to change a logo or tweak a style, you just update the template, and all SMTP channels using that template will automatically reflect the change.

The **Manage Templates** action is available in the Channels node and all its descendant nodes.

Customization and Upgrades

You're not limited to a single template; you can have multiple to suit your organization's diverse needs. If you decide to modify a factory template or built-in channel, those changes will stick around even after a server upgrade. And if you ever want to revert to the original settings, you can do so at any time.

Flexibility in Configuration

Feel free to edit built-in items directly or to copy existing templates and SMTP channels for quick modifications. You also have the option to create templates and SMTP channels from scratch, giving you maximum flexibility in how you manage your SMTP log delivery.

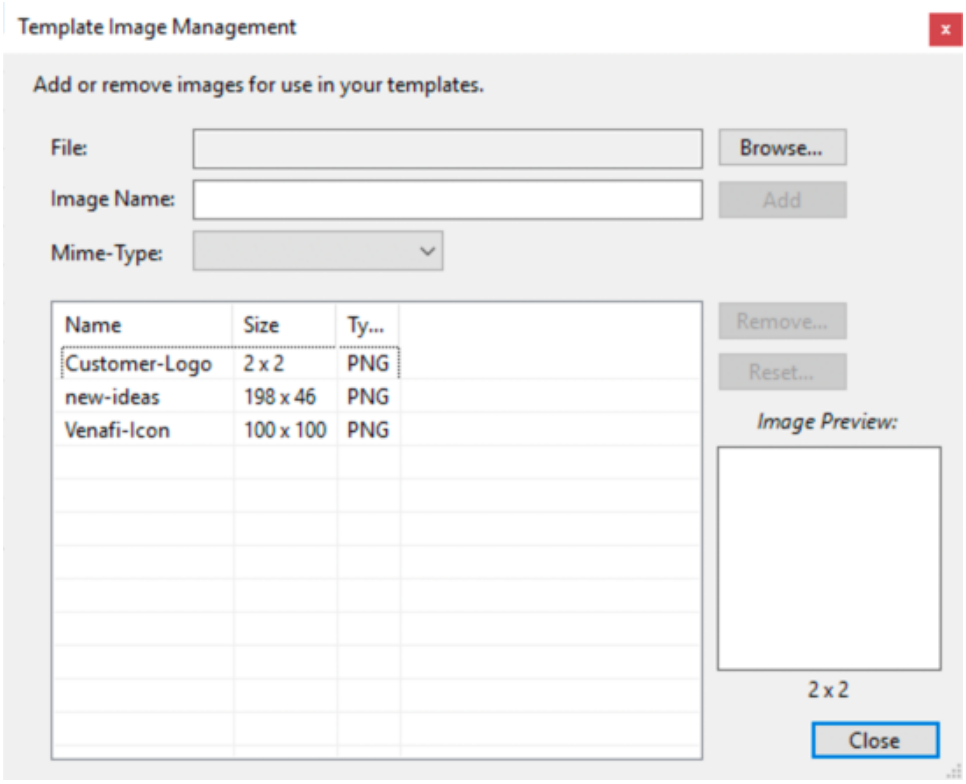
Managing logos and images used in email templates

Venafi Configuration Console (VCC) centralizes the management of images used in email templates. This makes it easy to add or remove images across all templates and messages where those images appear.

Before you start, ensure you have the images you want to use saved on the local system—either on the Venafi server for VCC or on your workstation if you're using the MMC snap-in.

To manage images for use in email notifications

1. In Venafi Configuration Console (VCC), go to **Tools** > **Channels**.
2. In the Actions panel, click **Manage Images** to open the Template Image Management window.



To add a new image:

1. Click **Browse** to locate the image file.
2. Click **Open**.
3. Verify the **Image Name** and the detected **Mime-Type**.

   The Image Name is what you'll use in templates, so make it short but descriptive.
4. Click **Add**.

To remove an image:

1. Select an image from the list.
2. Click **Remove** and then **Yes**.

If you remove a factory image and don't replace it, it will be restored the next time you refresh the Logging node.

To replace an image:

1. Select the image you want to replace and note the value in the **Name** column.
2. Click **Remove**.
3. Click **Browse** to locate the new image and click **Open**.
4. Replace the **Image Name** text with the value you noted earlier.
5. Verify the **Mime-Type** and click **Add**.

If you have replaced a Venafi-provided image, your change will be preserved when you upgrade Venafi Platform.

The factory image `Customer-Logo` is a transparent two-pixel square image that is pre-inserted in the default email template. If you replace this with your organization's logo, your logo will automatically appear at the top of the default message template. If you leave it as is, it won't cause any issues since it's transparent.

To reset a factory-provided image to its default state:

1. Select an image in the list.
2. Click **Reset**.

   The Reset option is only available for Venafi-provided images.

   You can't reset images not provided by Venafi. If the **Reset** button is disabled, the image you selected is not a Venafi-provided image.
3. Click **Yes**.

About SMTP templates for email notifications

Email templates in Venafi Platform serve as a wrapper for your message content, providing a consistent header, footer, style, and structure. The power of using templates is that a single change can update all messages based on that template.

Where to Find Templates

Templates are managed within the Venafi Configuration Console (VCC) under **Tools** > **Logging** > **Channels** or any of its descendants.

Customizing Templates

Venafi Platform comes with a built-in email template that serves as the default for all SMTP notifications. You have several options for customization:

- Edit the built-in template directly.
- Duplicate the built-in template and edit the copy.
- Create a new template from scratch.

For more information, see "Editing SMTP message templates" on page 457.

Setting the Default Template

If you have multiple templates, you'll need to designate one as the default. This is the template that will be used when no other template is specified in the SMTP channel object.

Preservation During Upgrades

SMTP templates are safeguarded during system upgrades. Any changes you make will be retained when you upgrade to a newer version of Venafi Platform.

Resetting to Default Configuration

If you've modified the built-in template and wish to revert to the original settings, you can easily reset it to its out-of-box configuration.

Editing SMTP message templates

If you want to change the templates used to send SMTP messages, you'll need to go to the Venafi Configuration Console (VCC) (or use the Tools MMC snap-in).

To open the template editor

1. In VCC, go to **Tools** > **Logging** > **Channels**.
2. Click **Manage Templates** in the actions panel.
3. Do one of the following:
    - To modify an existing template, click its name, then click **Edit**.
    - To edit a copy of an existing template, click its name, click **Duplicate**, and then click **Edit**.
    - To create a new template from scratch, click **New**.

Using the Template Editor

The template editor is a robust tool for crafting both HTML-based and plain text message templates. Both versions of the message are sent to recipients; their email system determines which version of the message to display.

You can edit the template name and author in the bottom right corner of the Template Editor.

Working with macros, images, and variables

There are three types of dynamic content used in the Template Editor: Macros, images, and variables.

Macros

Macros are keyword-based commands enclosed by a single `$` symbol. They pull system information into notifications. For example, `$IdentityEmail[<PrefixedUniversal>]$` would insert the corresponding certificate owner's email.

Macros are available in the menu across the top of the Template Editor. Click **Documentation** to see reference documentation for the selected macro. (To hide the help window, click **Documentation** again.)

Images

Images are variables enclosed by three `$$$` symbols and are *always* the value of the `src=` attribute. For example: `<img src="$$$Venafi-Icon$$$" />`

To learn how to manage images, see "Managing logos and images used in email templates" on page 453

To insert an image into the message at the current position, click the logo title, then click **Insert Image Reference**.

Variables

Variables are units of dynamic content that will be replaced with specific content defined in the individual SMTP channel settings. When you have multiple templates, you'll see a couple of different groupings of variables. *Shared* variables are variables that exist in all templates. Conversely, *custom* variables only exist in a subset of templates.

When possible, we recommend you use shared variables as much as possible. Using shared variables makes your templates more useful because they can be used by emails that use any of the templates. If you use custom variables, you need to make sure the message settings in the SMTP channels match the variables of their templates.

In the Template Editor, you create and use variables by surrounding text with three `$$$` symbols. For example, this is a shared variable called title: `$$$Title$$$`.[1]

For example, if you have a detailed internal knowledge base, and you want to provide a link to different KB articles for different SMTP channels, you could create a variable called `$$$KbUrl$$$`. You could then define that URL for each SMTP channel in the Edit Message window. [2]

When you create variables, you can see them in the Detected Variables panel. On the right of the detected variable name you can see if the components were found in the HTML or Plain text versions of the message. To find the component's location in the email, click the name in the variable list, then click **Go to variable**.

One notable feature is the ability to nest variables. This means a variable can contain one or more other variables, allowing you to create reusable combinations of variables. If the system detects a recursive variable (a loop where a variable contains itself somewhere in the definition), it will output the loop five times, and will then stop generating. This helps you visually identify cases of recursive variables so you can hopefully fix them before the broken messages get sent to your users.

HTML and plain text messages

SMTP messages should be created in both the HTML and Plain text tabs. Depending on the recipient device and software, either the HTML or plain text version of the message may be shown to users. For example, if the SMTP channel target is a modern email system, the HTML version would likely be displayed. However, if the SMTP channel target is an SMS destination, the plain text version would be displayed.

In the HTML tab, you can use standard HTML syntax, including CSS in the style element, as well as inline CSS. The Preview window shows you a visual rendition of what the message will look like.

---

[1]The syntax for variables, macros, and images is CASE-SENSITIVE.
[2]Remember that you will need to specify this value on every SMTP channel that use this template. In this example of a country-specific URL, another reasonable approach would be to create separate templates for different regions, and just use the actual URL in the template code, so that you don't have to edit every SMTP channel to include the correct URL, and then assign the correct template to the correct SMTP channels.

Individual SMTP channels can be set to only deliver plain text versions, if needed. This is useful, for example, if the resulting email will be automatically processed by another system where a plain text version is preferable.

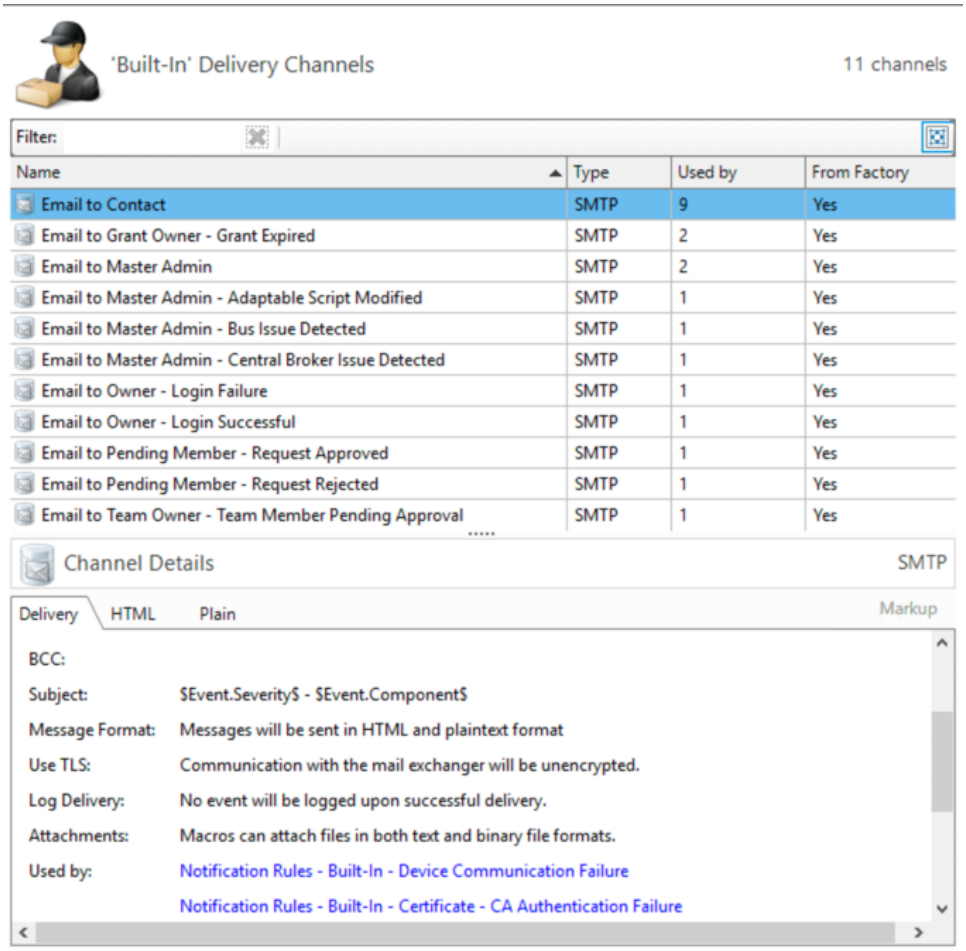
Saving your changes

Make sure you save your changes before you close the window. Once your changes are saved, all SMTP messages that use this template will be sent with the updated settings.

Built-in SMTP channels

The Channels node in Venafi Configuration Console (VCC) includes about 45 built-in channels, all but one of which are SMTP channels.

Expand the folders in the Channels node to see the sub channels. Notifications are grouped by product area.



The table shows the defined delivery channels in this folder. The bottom panel shows details about the channel settings. In the case of SMTP channels you can also see the HTML and plain-text renderings of the message.

The Delivery tab shows how the message will be delivered, the object configuration settings, as well a list of the notification rules that are connected to the channel.

For SMTP objects, the actions panel allows you to set the **Properties**, or you can click **Edit Message** to customize the contents of the notification.

SMTP channel properties

When you click the Properties action you can edit the settings that control how messages are sent. The following table shows the properties and their descriptions. Note that all text fields support macros.

SMTP Options

Field	Accepts Macros	Description
Description	No	A plain text description of the purpose of the SMTP channel.
Host	No	Hostname or IP address of the SMTP server. Trust Protection Platform Channel drivers support both IPv4 and IPv6 connections. If a hostname is specified, only the first resolved address associated with that name is used. You can append the port number to the host. For example: *<hostname>:25*.
Credential	No	Username credential required to authenticate with the SMTP server. Configure this option only if SMTP authentication is configured on your SMTP server. Otherwise, all notifications routed through this Channel object will fail.
Sender	Yes[1]	Name that appears in the From: line for all messages sent from this SMTP Channel object. Some SMTP servers require this field to be a valid email address. If this is required by your SMTP server, make sure you provide a valid email address, such as username@yourcompany.com.
Recipient	Yes	Specifies the recipients who should receive this notification. Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
CC	Yes	Specifies the recipients who should be copied on this notification. Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
BCC	Yes	Specifies the recipients who should receive a blind carbon copy of this notification. This field allows you to send the notification to a distribution list or group, but prevent "reply all" messages from being sent to the entire group.

[1]Use caution if you use a macro here, as it can lead to issues. For example, if the macro can't resolve, email messages may not get sent.

Field	Accepts Macros	Description
		Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
Subject	Yes	This will be the subject of the sent message.
Attachments	N/A	Some notification types can include files as attachments. Select **Allowed** to send attachments. Use the drop-down to specify the types of files that can be attached. If needed, you can ensure that items are not embedded, only attached. For example, a notification of a certificate renewal can include an attachment that contains the renewed certificate data.

Field	Accepts Macros	Description
Use TLS	N/A	Configures the SMTP channel driver to use Transport Layer Security (TLS) to send SMTP notifications. Select this option only if your SMTP server is configured to support TLS. Otherwise, all notifications routed through this Channel object will fail. SMTP channels can communicate with SMTP servers with or without authentication. SMTP channels can send events through servers that require SMTP authentication as long as a valid username credential is referenced in the SMTP channel configuration. If the username credential is configured, the SMTP channel *always* attempts SMTP authentication when connecting with the relay host. If the authentication failed, the SMTP driver logs an *SMTP Message Failure* event. If the SMTP channel successfully authenticates with the SMTP server and sends the message, it logs an *SMTP Message Success* event.
Log Delivery	N/A	The setting to manage SMTP events regarding delivery success or failure. *No*: Discard log events. *Yes*: Log email notifications. For example, the driver fails to connect to the SMTP server. If available, additional information appears in the exception details from the SMTP server. This information is helpful in troubleshooting connectivity and configuration issues.
Send Plaintext messages only	N/A	When *not* checked, messages are sent in both HTML and plain-text, and the client determines how to display the message. However, if you never want HTML messages sent to this channel, you can check this option.

Editing SMTP channel message contents for email notifications

The SMTP message editor in Venafi Configuration Console allows you to customize the value of the variables defined by the SMTP message template. It provides a list of variables on the left, and space on the right to define the variable value. You can insert macros into any variable value using the macros at the top of the page.

Specify a template

The **Use Template** drop-down allows you to choose **which template will be used to send the email** when you have multiple templates.

Preview the message

Click the **Show Preview** link to see a rendered version of the SMTP message.

At the top of the Message Preview window, you can select which template to use for the preview. You can also click the **View** button to switch between the HTML-based and plain-text renderings of the message.

Define variable values

For each variable in the list, you can specify the variable's value using any combination of text, HTML markup, and macro content.

Each variable name has an icon. Icons with a green check have a value defined for that variable. Icons with a red X *do not* have a value defined for that variable.

If a variable doesn't have a value defined, it will be excluded from the resulting message. For example, The `CallToAction` variable is displayed in the built-in email template as text in a `div` element on a colored background. If the variable value is empty, the `div` element itself is included in the message, but because it does not have any content it isn't visible.

Using macros in the SMTP Message Editor

Variable values can include text and macros. They can even include HTML markup. For example, the built-in channel *'Email to Pending Member - Request Rejected'* has the following default value for the `Details` variable:

```
<p><b>Rejection Comment:</b> $DictionaryKey[$Event.Data$, "Comment"]$</p>
<p><b>Rejected by:</b> $Identity[$Event.Text1$]$</p>
<p><b>Requested by:</b> $Identity[$DictionaryKey[$Event.Data$, "Suggested By"]$]$</p>
```

In this example, notice the combination of macros, text, and HTML markup.

> **NOTE** When HTML formatting is included in a variable's value, the markup is stripped out for plain-text messages.

To add a macro to a variable's value, use the Macro menu at the top of the editor. Use the **Documentation** button to learn more about the highlighted variable. (Use the **Documentation** button again to hide the help window.)

Use the **Toggle Word Wrap** button to make long variable values easier to read and edit.

When you are doing making changes, be sure to **Save** your changes.

Message delivery failures

If the SMTP channel driver can successfully send an event message, it logs an *SMTP Message Success* event. Otherwise, the SMTP channel driver logs a *SMTP Message Failure* event for the following reasons.

- Configuration errors in the SMTP Channel object. The SMTP channel driver does not buffer events that are undeliverable because of a misconfiguration.
- Connect issues with the SMTP server. To help you troubleshoot the message failure, SMTP Message Failure events provide the exception details returned from the SMTP server.

Adaptable Log channel

The Adaptable Log Channel driver lets you implement custom actions in response to events that are logged by Trust Protection Platform.

This driver can perform virtually any programmatic task in response to the logging of an event. The Adaptable Log Channel driver can interface directly with ITSM and/or SIEM solutions to create support tickets, change requests, security incidents, and so forth.

For applications that require access to the Venafi Web SDK, Trust Protection Platform can manage authentication for you automatically, reducing the overhead in your PowerShell script. When implemented, each time your script is called, Trust Protection Platform requests a new token automatically. Each new token is associated with both the specified user and with the referenced application ID. After the script finishes running, Trust Protection Platform revokes the token automatically. To get started, see "Adaptable Log Channel prerequisites" on page 467.

Adaptable Log Channel prerequisites

Before you configure a Venafi Adaptable Driver object in Trust Protection Platform, review the following prerequisites:

- Review the Adaptable Log Channel design to determine the Trust Protection Platform logged events to which you want the driver to respond.
- To work effectively with any Venafi adaptable solution, you must have some working knowledge of PowerShell scripting, or you must have equivalent experience with a scripting language similar to PowerShell.

- Identify who will write the logic for the PowerShell functions in the Adaptable Application driver script.

  Will you write the logic yourself, or will you delegate the task to an internal development resource, Venafi Professional Services, or someone else?

- Install Windows PowerShell 3.0 or later.
- Install .NET 4.8 or later.

What's next?

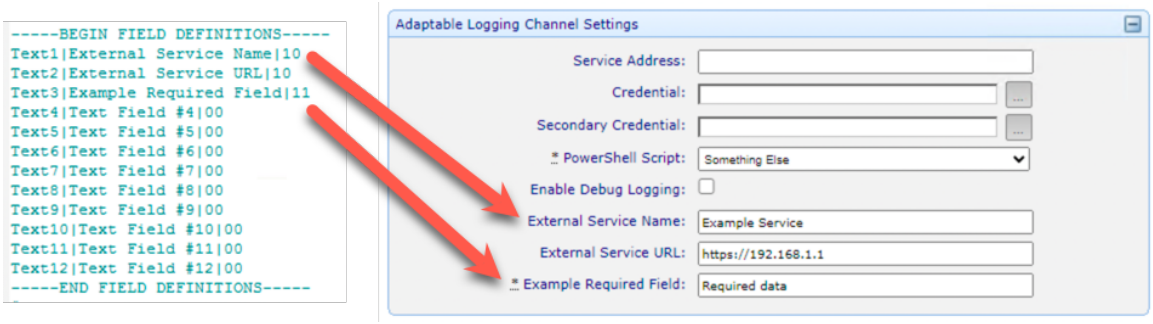
After you've completed the Adaptable Log Channel prerequisites, see "Configuring the Adaptable Log Channel object" on page 472.

About the Adaptable Log Channel PowerShell script

The Venafi Adaptable Log Channel, like the other Venafi Adaptable Drivers, uses PowerShell scripts that contain functions that can be used to perform virtually any programmatic task in response to a logged Venafi Platform event.

> **TIP** When creating new PowerShell scripts for use with adaptable drivers, keep in mind that the file name is used to identify your script from within the associated object (and within the policy for the Adaptable Application driver) in Trust Protection Platform. Using logical names can help you and other administrators recognize the purpose and intent of each script.

The Adaptable Log Channel configuration provides a common set of variables for use in Logging. However, if you need to pass unique or additional data to your script or third-party application, you can define up to twelve additional text fields. You do this by simply modifying the **Begin Field Definitions** section of the Adaptable Log Channel PowerShell script.



NOTE About macros: It's important to note that the Service Address field **does not accept macros**. You must use a custom field instead. Please be aware that certain macros are designed to function exclusively within workflows. Use the Macro Evaluator along with sample data to help you understand how macros will be processed for your use case.

Each field definition has three parts:

Field Name| *Field Label*| *Flags*

1. Field Name: Must be `Text1` through `Text12`. Do not modify these values.
2. Field Label: Type the name that you want to appear on the Adaptable Log Channel application object settings page.
3. Flags: Using the numeric values of `0` (to mean false) or `1` (to mean true) for each of the following options (in order):
    - Enabled: Use to enable or disable a field.
    - Mandatory: Use to indicate whether the field must be completed, or is optional. When set to true, this option adds an asterisk (*) next to the field label to let the user know that it is a required field.

EXAMPLE Suppose you want to add two required fields to capture an external logging application name and URL. Using a text (or PowerShell script) editor, you would open your PowerShell script file (which must be in the `[drive]:\\Venafi\Scripts\AdaptableLog\` folder). You would then edit the field definitions in the header section to include new fields like in the example below, then set and set values for the available flags:

```
----------BEGIN FIELD DEFINITIONS--------
Text1|External Log Provider Name|11
Text2|External Log Provider URL|11
Text3|Text3|00
Text4|Text4|00
Text5|Text5|00
Text6|Text6|00
Text7|Text7|00
Text8|Text8|00
Text9|Text9|00
Text10|Text10|00
Text11|Text11|00
Text12|Text12|00
```

When you are finished, you save your changes to the PowerShell script. When you open Policy Tree, your new fields appear on the Adaptable Log Channel objects.

IMPORTANT The header is required! The Powershell script will not work if the following header information is removed:

```
---- BEGIN FIELD DEFINITIONS ----
```

To create (or edit) Adaptable Log Channel data fields

1. Open your Adaptable Log Channel PowerShell file using a text (or PowerShell script) editor.

   Adaptable Log Channel PowerShell script files must be stored in the `\Venafi\Scripts\AdaptableLog\` folder.

2. Locate the **Begin Field Definitions** section and determine where you want to place your new field.

3. On the line where you want to define your new field, type the new field label and then set the appropriate flags.

   For example:

```
Text1|External Log Provider Name|11
Text2|External Log Provider URL|11
```

4. When you are finished, save the file and close it.

Your new field should appear on both the Adaptable Log Channel object page in Policy Tree as well as on the adaptable channel object in Venafi Configuration Console (VCC).

Example: creating a ServiceNow incident for expiring certificates

The Adaptable Log Channel driver lets you implement a custom action in response to events that are logged by Trust Protection Platform. The following sample code demonstrates calling the ServiceNow API to create an incident when a certificate is nearing expiration.

This sample script assumes that the Adaptable Log Channel object to which this script is assigned is targeted by a notification rule that executes whenever the *Certificate Monitor - Certificate Expiration Notice* and/or the *Certificate Monitor - Certificate Expiration Escalation Notice* events are logged.

```
function Perform-Action
 {
  Param(
   [Parameter(Mandatory=$true,HelpMessage="General Parameters")]
   [System.Collections.Hashtable]$General,
   [Parameter(Mandatory=$true,HelpMessage="Event Detail Parameters")]
   [System.Collections.Hashtable]$Event,
   [Parameter(Mandatory=$true,HelpMessage="Extra Field Parameters")]
   [System.Collections.Hashtable]$Fields
  )
  $passwd = ConvertTo-SecureString $General.UserPass -AsPlainText -Force
  $cred = New-Object System.Management.Automation.PSCredential($General.UserName, $passwd)
  $url = $General.ServiceAddress + "/api/now/table/incident"
  $body = @{
   "category"="request";
```

```
    "short_description"=$Fields.Text1;
    "description"=$Event.Description;
    "comments"="Created by Venafi Trust Protection Platform Adaptable Log Channel using the ServiceNow API";
    "impact"=3;
    "urgency"=3;
    "work_notes"=$Fields.Text2;
    "priority"=3; # 1=critical, 2=high, 3=moderate, 4=low, 5=planning
    "contact_type"="self-service";
    "caller_id"="68f87b0bdb97a2009dfaf91ebf9619e9"
  } | ConvertTo-Json
    $resp = Invoke-RestMethod -Uri $url -Credential $cred -Method Post -Body $body -ContentType "application/json"
    $sys_id = $resp.result.sys_id
    return @{ Result="Success"; Updates=@{"Description"="ServiceNow Incident ID=" + $sys_id} }
}
```

For another example of simplifying authentication to the Web SDK, take a look at this Venafi Cool Solutions article.

Configuring the Adaptable Log Channel object

Creating and configuring an Adaptable Log Channel object is similar to creating any other application object, except that you must specify the PowerShell script you want to use. However, in the case of Adaptable Log you can also make these configuration settings in Venafi Configuration Console or in the Tools MMC snap-in.

> **NOTE** Before you attempt to create CA template, device, or application objects, you must enable the *create* permission under the folder where you want to create the new object. For more information, see "Permissions overview" on page 713 in the *Administration Guide*.

To create and configure a new Adaptable Log Channel object

1. In Venafi Configuration Console (VCC) browse to the **Tools** > **Logging** > **Channels** node.
2. In the Add Channels section of the Actions panel, click **Adaptable**.
3. Provide the name you want to use for the new Adaptable Log channel, then click **Add**.

4. In the channel settings, configure the following:

   a. In the **Service Address** field, type the network address (e.g. URL) of the service with which the Adaptable Log Channel driver will interact.

   b. Click **Credential** to browse for the location of the credential object that you want to use to authenticate.

   > **NOTE** If you're connecting to the Venafi Web SDK, leave this field empty since you'll be specifying a credential in the WebSDK OAuth Token Configuration settings.

   Credential objects store the credentials Trust Protection Platform uses to authenticate with devices, applications, and CAs. The stored credential may be a password, a user name and password, a certificate, or a private key.

   > **NOTE** The user account you select must have *Read* and *Write* access to the Temporary, Private Key, and Certificate directories.
   >
   > For more information, see "Working with system credentials" on page 909the Managing system credentials section of the *Venafi Trust Protection Platform Administration Guide*.

   c. (Optional) (Conditional) If you need to select another credential, then from the **Secondary Credential** field, select a username, certificate, password, or CyberArk credential object.

   > **TIP** Use this option to avoid having to hard code additional credentials in your script or having to utilize other solutions outside of Trust Protection Platform.

   d. From the **PowerShell Script** list, select your custom PowerShell script.

   Your custom scripts must be in the `\Venafi\Scripts\AdaptableLog\` folder in order to appear in this list.

   > **BEST PRACTICE** You should consider placing Adaptable scripts on all of your Trust Protection Platform servers so that you don't have to worry about the roles those servers are performing.
   >
   > Adaptable Log Channel scripts *must* be placed on both the server that's hosting the Venafi web-based console, and any other servers where you're running Venafi's Log servers. For both the Adaptable CA and Adaptable Application drivers, PowerShell scripts *must* be placed on the Venafi server that hosts Policy Tree, as well as on processing engines that are used for enrolling or provisioning work.
   >
   > For an explanation of the various Trust Protection Platform administration consoles, see "About Venafi Trust Protection Platform administration consoles" on page 3.

e. (Optional) If you want to enhance troubleshooting capabilities of your Adaptable Log ChannelAdaptable Flow, select the **Enable Debug Logging** check box.

For information about how enabling this option works with the PowerShell script, see "About debug logging" on page 477 in the Adaptable Log Channel Adaptable Flow PowerShell script reference.

5. (Optional) If your application will connect to the Venafi Web SDK, then complete the **WebSDK OAuth Token Configuration** settings:

Setting	Description
OAuth Token Application ID	Enter the application ID of the *API application integration* you should have created previously, as described in "Adaptable Log Channel prerequisites" on page 467.
OAuth Token Credential	Select the username credential of the service account that has been granted access to the Client ID of the API Application. See "Adaptable Log Channel prerequisites" on page 467. In this context, the username credential identifies the user (identity) for whom the token is being requested. It also verifies whether you have the required permissions within your organization to enable the script to authenticate as the selected user. This security measure prevents users from impersonating another user.
OAuth Token Scope	(Optional) Enter one or more of the scopes assigned to your API application. For example, Certificates: Manage. Leave this field blank if you want to include all defined scopes. To learn more about scopes and restrictions, see Token Auth scope in the Developer's Guide.

NOTE If your application is not connecting to the Web SDK, leave all of these fields blank.

6. (Conditional) If your script includes customized fields, enter the desired static text or macro commands.

Refer to the sample in the topic, "Example: creating a ServiceNow incident for expiring certificates" on page 471.

For more information about Venafi's macros, see Macro commands in the *Macro Guide*.

7. When you're finished, click **OK**.

IMPORTANT If you make changes to the PowerShell script used by an Adaptable Log Channel, you must open the corresponding log channel object and click **Save** to force the driver to re-read the script, which will happen almost instantly.

Protecting against unapproved changes to Adaptable Log Channel scripts

Venafi's Adaptable drivers—such as Adaptable CA, Adaptable Application, Adaptable Bulk Provisioning, and Adaptable Log Channel—rely on PowerShell scripts stored in the *\Venafi\Scripts\AdaptableDriverName* directory on Trust Protection Platform servers. To ensure the integrity of these scripts, Trust Protection Platform supports signed scripts.

Because other people might have access to the server that is running Trust Protection Platform, they could modify your PowerShell scripts without your knowledge, either accidentally or intentionally. However, with signed scripts, any modifications made to the script will result in a failed signature validation, and the script will not be executed.

To protect against unapproved changes to your scripts, Trust Protection Platform monitors PowerShell script files that are being used by existing Adaptable objects. If a new script is used or a PowerShell script is modified on the file system, Trust Protection Platform displays a warning and you'll need to re-validate the script.

This security feature helps to prevent potentially harmful modifications to your scripts from being run.

IMPORTANT Because of this security feature, following an upgrade to Trust Protection Platform, you must take specific steps on all existing Adaptable objects in order for them to be re-enabled. Refer to the documentation for each Adaptable driver for details.

To use VCC to re-enable an Adaptable Log Channel driver after a script change

1. From Venafi Configuration Console (VCC), navigate to the **Tools** > **Logging** > **Channels** node.
2. Locate the adaptable log channel whose script was modified.
3. In the **Actions** panel, click **Properties**.
4. Click **Save**.

To use the web console to re-enable an Adaptable Log Channel driver after a script change

1. From the Platform menu bar, click Policy Tree.
2. From the **Tree** drop-down menu, select the **Logging** tree.
3. Expand the **Channels** folder and click your existing **Adaptable Log Channel**.
4. On the **Adaptable Channel** > **Settings** tab, click **Save**.

PowerShell script reference for Adaptable Log Channel

This section documents all available PowerShell functions for use with the Adaptable Log Server driver. PowerShell scripts are stored in the \Venafi\Scripts\AdaptableLog folder.

The input parameters and response format for each function is predefined. All functions receive a set of general parameters, whereas those parameters that are *specific* to the function are only passed to it.

> **DID YOU KNOW?** To prevent vulnerabilities, the PowerShell scripts are stored on the Trust Protection Platform server. While it might have been more convenient to allow downloading the script, storing the scripts on the Trust Protection Platform server prevents potentially harmful scripts from affecting the server. Only privileged users on your Trust Protection Platform server can access scripts.

You must ensure the same version of all your Adaptable Log Server scripts are on all servers in the cluster that have the WebConsole component installed. For this reason, it is wise to include a script version number in the file name, so you can easily check to see that the same version of the script is installed on all servers in the cluster.

NOTE To work effectively with any Venafi adaptable solution, you must have some working knowledge of PowerShell scripting, or you must have equivalent experience with a scripting language similar to PowerShell.

A sample script is provided in the `\Venafi\Scripts\AdaptableLog\Samples` folder. Only files that are in the main `\Venafi\Scripts\AdaptableSSHManagement\` folder can be selected in an Adaptable Log object in Policy Tree or VCC. Files in all sub-folders are ignored.

BEST PRACTICE When customizing (or creating a new) PowerShell script, keep the following security best practices in mind:

- Avoid hard-coding credentials into your PowerShell scripts.
- Only include code in functions that relate to the task they are designated to perform.
- Scripts should not do anything that could alter the integrity or availability of the local Windows system (the system hosting Trust Protection Platform).

IMPORTANT If you make changes to the PowerShell script used by an Adaptable Log Channel, you must open the corresponding log channel object and click **Save** to force the driver to re-read the script, which will happen almost instantly.

About debug logging

When a user has requested debug logging by checking **Enable Debug Logging** for Adaptable Log Channel, the driver sets a global variable called $DEBUG_FILE whenever it executes a PowerShell function. So your PowerShell script should reference the value of the $DEBUG_FILE variable to decide whether or not to log information for troubleshooting purposes. The value the driver assigns to the $DEBUG_FILE variable is a recommended file path name on the Trust Protection Platform server for use when logging events to a file. The file name is designed to be unique to the instance of the Adaptable component so as to avoid conflicts when multiple scripts are running at the same time and writing to the log file. If the recommended file name is used, the resulting log file appears in the `<Venafi Home>\Logs` directory by default (e.g. `C:\Program Files\Venafi\Logs`).

For information about where Enable Debug Logging is configured for Adaptable Log Channel, see "Configuring the Adaptable Log Channel object" on page 472.

About hash tables

Data is passed to (and returned by) each function using hash table data structures.

A *general* hash table, which includes a common set of data, is passed to available functions. A *specific* hash table, which includes data that is applicable specifically to the function, is passed to functions that require additional data. All functions must return a single hash table that includes a *result* along with any other variables that the function is required to return.

CAUTION Functions must not return errors; rather, they must throw exceptions in the same way that actual PowerShell errors do. The Adaptable Log Channel driver treats exceptions thrown by a PowerShell function as a fatal error and then halts processing.

Perform-Action function

Use the *Perform-Action* function to perform a specific action in response to the logging of an event by Trust Protection Platform.

Variable Name	Data Type	Description
AuxPass	String	The password portion of the Secondary Credential when a user name or a password credential is assigned, or the PKCS#12 password when a certificate credential is assigned
AuxPfxData	Byte Array	A PKCS#12 byte array that contains a client certificate and private key when a certificate credential is assigned as the Secondary Credential
AuxUser	String	The user name portion of the Secondary Credential when a user name credential is assigned
OAuthAccessToken	String	OAuth token passed to the PowerShell script. Tokens are passed only after you've provided the required information in the *WebSDK OAuth Token Configuration* settings of the Adaptable object. See "Configuring the Adaptable Log Channel object" on page 472. **How it works** When used, each time your script is called, Trust Protection Platform requests a new token automatically. Each new token is associated with both the specified user and with the referenced application ID. After the script finishes running, Trust Protection Platform revokes the token automatically. To get started, see "Adaptable Log Channel prerequisites" on page 467.
	String	The network address (e.g. URL) of the service with which the Adaptable Log Channel driver interacts.
UserName	String	The user name portion of the user name credential assigned to the Adaptable Log Channel instance. Used to authenticate with a remote system or service.
UserPass	String	The password portion of the user name credential assigned to the Adaptable Log Channel instance. Used to authenticate with a remote system or service.

Variable Name	Data Type	Description
ID	String	The event's Event ID field as defined in the logging application LSC file.
Name	String	The event's Description field as defined in the logging application LSC file.
Description	String	The event's Readable Log Text field as defined in the logging application Log Schema Channel (LSC) file.
Severity	Integer	The event's log level: ■ 1 = Emergency ■ 2 = Alert ■ 3 = Critical ■ 4 = Error ■ 5 = Warning ■ 6 = Notice ■ 7 = Info ■ 8 = Debug For more information, see About logging thresholds in the Log Server Administration Guide.
ServerDate	DateTime	The month, day, year, hour, minute, second, and millisecond (UTC) that the logging server received the event. The date and time displayed are specific to the Locale defined on the Log server.
ClientDate	DateTime	The date and time (UTC) that the logging application generated the event.
Component	String	The DN of the object–i.e., the application, CA, certificate, workflow ticket, device, or credential–that triggered the event.
Grouping	Integer	An ID that can be used to identify related events.
Text1	String	The value of this field depends upon the event. It can contain any text string up to 255 characters.

Variable Name	Data Type	Description
Text2	String	The value of this field depends upon the event. It can contain any text string up to 255 characters.
Value1	Integer	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
Value2	Integer	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
Data	ByteArray	The value of this field depends upon the event. The maximum data size is 1536 bytes.

Variable Name	Data Type	Description
Text1 *through* Text12	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.

Return	Data Type	Description
Result	String	Shows "Success" to indicate the non-error completion state.
Updates	String	(Optional) Hash table of attribute name-value pairs pertaining to the Event.Component that specify what the driver will update when the result is "Success."

File channel

The File channel collects log server events directly to a file in either the CSV format or the translated format (default setting), which writes the log in a human-readable format. The log data is defined in the corresponding event definition.

CSV files simply contain the event data; consequently, they are difficult to decipher. However, because these comma-delimited files maintain a consistent field structure across events, you can import these files into spreadsheet programs like Microsoft Excel to query the log data.

The following is a sample from a CSV log file:

```
2130706433,1250570028,1250570028,\VED\Engines\Jupiter,917507,Info,0,\VED\Engines\Jupiter\
TLS Protect,,0,0,,
 2130706433,1250570029,1250570029,\VED\Engines\Jupiter\TLS Protect,1245202,Info,0,,,10000,0,,
```

```
2130706433,1250570029,1250570029,\VED\Engines\Jupiter\TLS Protect
,1245197,Info,0,\VED\Policy\Import\cert1.venafi.com,10/05/2009 03:49:24,0,0,,
```

On the other hand, translated log files are more human-friendly. They can be visually scanned for content. However, it is difficult to generate reports from translated log files because there is no delimited field structure. They get their main content from the Translation field in the event definition. (In the event definition table view, this field is just called Log.)

The following is a sample from a translated log file:

```
127.0.0.1, 17/08/2024 22:17:41: EncryptionDPAPI initialized successfully.
127.0.0.1, 17/08/2024 22:17:42: The Venafi Encryption Trust Protection Platform service manager for the engine Jupiter is running in 32 bit mode.
127.0.0.1, 17/08/2024 22:17:42: The engine \VED\Engines\Jupiter is loading the service module \VED\Engines\Jupiter\TLS Protect.
127.0.0.1, 17/08/2024 22:17:42: The certificate management service module for the engine Jupiter is examining certificates for expiration.
127.0.0.1, 17/08/2024 22:17:42: The certificate management service module for the engine Jupiter is examining certificates for notification.
127.0.0.1, 17/08/2024 22:17:42: The certificate manager for Jupiter has found 10000 certificates for renewal expiration consideration.
127.0.0.1, 17/08/2024 22:17:42: The certificate manager for Jupiter has found 0 work to do requests for consideration.
```

The Venafi Log server can use the file channel to create specialized log files for specific types of events.

WARNING! If you are using a file channel, you should strongly consider only using a *single* log server. If you are using multiple log servers, and if your file output is saved locally on each Venafi server, you will have incomplete logs on each server. You would need to manually combine all log files for an accurate, complete log. If your file output is saved on a shared network drive, your log servers will constantly be competing to write to the file, which will result in errors and incomplete logs.

File channel requirements

The following list contains the requirements for file channels:

- To enable the Venafi Log server to log data to file, you must create and configure the File channel object in Trust Protection Platform. For information on creating the File channel object, see "Creating Channel objects" on page 442.
- The Log server must have full permissions to the log file directory defined in the File channel object.
- The space you need for your log file depends on a number of factors. These include, but are not limited to, how many events per second you are storing and how long you want to keep the data. As a general baseline, Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.

File channel configuration

As described previously, the File channel uses the event definitions to create CSV and translated log files. Depending on the channel settings, the file will be written in CSV format, or in the translated, human-friendly format. The event definitions contain the all the data used for the resulting logs which will be stored, in the case of File channels, to a text file. When you create a file channel, you can choose whether the data in the file will be written in CSV format.

To manage resources, a File channel accumulates data and writes it periodically, so there may be a short delay between the event and the target log file being updated.

You should figure out how you will ensure the target disk doesn't get too full. If the disk runs out of space, the log server can *not* operate. The amount of disk space you need depends on a number of factors such as the retention period and the volume of events. For example, daily validation checks and certificate monitoring generate many event log entries. A certificate renewal can generate about 10 events.

To configure a File channel

1. In Venafi Configuration Console (VCC), open **Tools** > **Logging** > **Channels** .
2. If the File channel already exists, locate it and click the **Properties** action.

   If you need to create a new File channel, click **File...** in the **Add Channel** section of the **Actions** panel, then give the channel a name.
3. Use the following table to configure the File channel .

Field	Description
Path/File	The directory and/or filename of the File channel log. Periodically the File channel driver saves the data to the log file. The event log name and location depends on one or more of the following factors: ◦ If no value is provided, the log file is written in the default log directory, and the file name will match the File channel name. For example, *\Program Files\Venafi\Logs\MyFileChannelForEvents.log*. ◦ If the value contains the path, but omits the file name, the file name will match the File channel name, and will be written in the specified location. For example, *MyFileChannelForEvents.log*. ◦ If the value omits the file extension, the File channel automatically appends *.log* to the filename. ◦ If the value has a valid directory and filename, the File channel records the event data in the Trust Protection Platform server file system at the specified location. ◦ If the specified directory does not exist in the file system, Trust Protection Platform creates the folder and log file.
Options > Translate raw events into text	A setting to control the way the File channel records events: ◦ When checked: Record translated events in the UTF-8 format. Include a byte marker at the beginning of the log file. Record only the event description based on the Event ID and matching Translation field from the event definition. Not suitable for reporting because the data uses an inconsistent field structure. ◦ When cleared: Use CSV to store untranslated log files. Omit the byte marker. Show only raw event data in a comma separated format. Suitable for reporting. Record untranslated events in this format: *SourceIP,ClientTime,ServerTime,Component,ID,Severity,Grouping,Text1,Text2,Value1,Value2,MIMEType,Data*

Field	Description
Create new log file at midnight	A setting to control log file size based on log date. ◦ When checked: At midnight, the previous day's data is saved to another file with the date and time appended. If that filename already exists (which could happen if the *Create new file when size reaches xx MB* option is also checked), a new file is created with a unique trailing numeric digit. New logs will continue to be written to the specified log file name. ◦ When cleared: The system doesn't use the current date to determine if a new log file should be created.
Create new file when size reaches *xx* MiB[1]	A setting to control the log file size based on file size. ◦ When checked: When the specified log file reaches the maximum size, the data is saved to another file with the date and time appended. New logs will continue to be written to the specified log file name. ◦ When cleared: The system doesn't use log file size to determine if a new log file should be created.
Delete existing log files older than *xx* days	A setting to purge old event log files. This is an important part of managing log files so they don't exceed the space available on the server. ◦ When checked: Any log files that match the *Path/File* setting above will be deleted if it is older than the specified number of days. If errors occur during the purge, the File channel driver records the events to the Windows application log. ◦ When unchecked: The system doesn't automatically delete logs. You will need another way to manage storage space on the log server.

4. Click **OK**.

Filter channel

The Filter channel allows the Venafi log server to block certain events or severity levels from being passed to other channels. This is primarily used for the default channel as a way to prevent unhelpful amounts of logging.

[1]This value is represented in mebibytes, which represents 2^20 bytes, or 1.049 megabytes.

To implement a Filter channel, you must configure the Filter channel as an intermediary channel between the event source and the final output channel. It is configured in Venafi Configuration Console (VCC).

To filter the default channel

1. In VCC, open **Tools** > **Logging** > **Channels**.
2. Create the Filter channel.
3. Configure the Filter channel's **Target Channel** attribute to point to the default log channel (this is usually the Default SQL Server channel).
4. Open the **Tools** > **Logging** > **Servers** node.
5. Click the log server, then click **Properties**.
6. In the **Default Channel** setting, specify your new Filter channel.
7. If you have multiple log servers, repeat the previous two steps for all logging servers. It's important that all log servers use the same default channel settings.

   For more information on the Log server configuration, see "Managing the log server" on page 429.
8. Open the **Product** node in VCC and **Restart** the **Logging** service.

Filter channel configuration

The Filter channel stores the information the system needs to block designated events or severity levels.

The following table describes the configuration settings for Filter channels:

Field	Description
Forward to	Specify the target channel that the Filter channel passes the unfiltered events to after it filters out the blocked events or severity levels.
Filter	Use as a text search to locate specific events.
Events	Event Filter options allow you to select which events you want to **block**.

Field	Description
	Checked events will be displayed below the Events selection box. These events will not be passed along to the target channel.
Severity	Severity Filter options allow you to select which event severity levels you want to **block**. Any events matching the selected severity settings will be blocked and will not be passed along to the target channel. For more info on severity levels, see "Event IDs and severity levels" on page 424.

TIP If you need to select a large number of events, or even whole groups of events to block, you may prefer to edit the filter object in web console. From the TLS Protect menu, click **Logs**, then locate the Filter channel you want to modify. Then click inside the **Events Blocked** panel.

The **Event Selector** window allows you to bulk select events. Items in the **Available** list are events that are *not blocked*. Items in the **Selected** list *are blocked*, and will appear as checked items in the VCC Filter channel editor.

What happens if I select items for both Events and Severity?

If you specify settings for both events and severity level(s), events that match *either* setting will be blocked and will not be passed along to the target channel.

SNMP channel

The Simple Network Management Protocol (SNMP) is a widely-used protocol designed for network management. It allows for the collection and organization of information about managed devices on IP networks, as well as for modifying that information to change device behavior. SNMP is commonly used in a variety of settings including corporate networks, service provider networks, and many others. It serves as a critical tool for network administrators to manage network performance, find and solve network issues, and plan for network growth.

In the context of Venafi Platform, the SNMP channel enables the logging server to send traps—essentially alert messages—that contain specific event data to an SNMP management system. This integration allows for real-time monitoring and automated responses to specific conditions in your encryption environment.

SNMP Versions and Compatibility

Venafi Platform supports three versions of SNMP:

- **SNMP v1:** The original version, which only supports IPv4 connections.
- **SNMP v2c:** An extension of SNMP v1, supporting IPv4, IPv6, or dual-stack configurations.
- **SNMP v3:** The most secure version, also supporting IPv4, IPv6, or dual-stack configurations.

Management Information Base (MIB)

For SNMP v2c and v3, Venafi Platform employs its own Management Information Base (MIB) file. An MIB is essentially a database that defines the properties of the managed object within the network that can be accessed via SNMP. In this case, the MIB file maps events to specific Object IDs (OIDs). These OIDs include both the event fields and readable log text, simplifying the task of searching for specific traps in your SNMP monitoring system.

Customizing the MIB

If you add, delete, or modify events, the MIB file will need to be regenerated to reflect these changes. Administrators also have the option to customize the MIB file by altering the Venafi Platform event schema. For more in-depth information, consult the section on "Customizing the Management Information Base" on page 493.

SNMP channel requirements

For proper communication between the Venafi Log Server service and the Simple Network Management Protocol (SNMP) host, you should consider the following requirements:

- You must have the Read Write permission to the Log Application objects.
- Port 162 must be open for User Datagram Protocol (UDP) traffic on all potential firewalls between Venafi Log server to the SNMP console. You can configure the firewalls accordingly.
- If the SNMP host only supports IPv4 traffic, you can configure the channel for SNMP v1. For more information, see "SMTP outbound server configuration" on page 451.

- Be sure the IIS bindings for Trust Protection Platform match the host SNMP settings. For example, if the SNMP host uses the IPv6 protocol, you can add a binding in IIS.
- If the SNMP host supports IPv4, IPv6, or a dual stack implementation, you can configure the channel for SNMP v2c or SNMP v3. Be sure the IIS bindings for Trust Protection Platform match the host settings.
- If there are multiple SNMP hosts that use more than one SNMP version, you must create a SNMP channel for each version.
- Ensure proper channel configuration. The SNMP driver does not buffer traps that are undeliverable because of a misconfiguration or a server failure.
- For each SNMP channel object, you must generate and distribute the *venafi.mib file* to the SNMP management console. Whenever events change, for example you upgrade to a new version of Trust Protection Platform, you can regenerate and redistribute the .mib file. For more information, see "Customizing the Management Information Base" on page 493.

SNMP Channel object configuration

The Simple Network Management Protocol (SNMP) Channel object stores the information the SNMP driver needs to send traps to an SNMP management system. You must have the Read and Write permission to the Log Application objects in the Logging Tree.

The following table provides a description of configuration settings for the SNMP Channel object.

Field	SNMP Version[1]	Description
Host	all	Hostname or IP address of the SNMP management system that receives Trust Protection Platform event notifications as trap messages. If a hostname is specified, only the first resolved address associated with that name is used.
SNMP Version	all	The setting that matches the host SNMP version. This setting works in conjunction with the matching section of additional configuration settings on the page. ■ *SNMP v1*: Uses a single trap OID for all events. Supports IPv4 connections between Trust Protection Platform and the host. ■ *SNMP v2c*: Generates traps with unique OIDs for each event. Uses its own MIB file with Trust Protection Platform event mappings to OIDs. The OIDs include the Trust Protection Platform event fields and descriptions so administrators can look for specific traps in their monitoring systems. Supports IPv4, IPv6, or IPv4/IPv6 dual stack configurations. ■ *SNMP v3*: Generates traps with a unique OIDs for each event. In addition to the same features as SNMP v2c, SNMP v3 provides encryption. Supports IPv4, IPv6, or IPv4/IPv6 dual stack configurations. **NOTE** If you change the MIB file, be sure to use the GenerateMIB utility to update the file. For more information, see "Customizing the Management Information Base" on page 493.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

Field	SNMP Version[1]	Description
Trap OID	v1	(Optional) The Object ID to associate with all traps that originate in Trust Protection Platform. The default is *1.3.6.1.4.1.28783.1.1*.The default OID was registered by Venafi for private use by enterprises. For more information, see http://www.oid-info.com/get/1.3.6.1.4.1.28783.
Message	v1	(Optional) The text that appears in the message body for all traps sent from this SNMP Channel object. Because SNMP specifications require that an SNMP packet can be no larger than 500 bytes, the message body is limited to 300 bytes. The SNMP driver simply truncates anything over 300 bytes. The SNMP notification message can be dynamically derived from the event using the Trust Protection Platform macro language.
Community	v1, v2c	Community string to access the SNMP management system.
Username	v3	Defines the username used to authenticate to the SNMP console when sending a trap.
Engine ID	v3	Defines the EngineID, used in the SNMP v3 protocol, to uniquely identify the Logging Server as an SNMP Engine.
Authentication	v3	Enables or disables SNMP v3 authentication.
Protocol	v3	Works in conjunction with **Authentication**. Defines the hashing algorithm, *SHA1* or *MD5*, used when SNMP v3 authentication is enabled. *SHA1* is the default hashing algorithm.
Passphrase	v3	Works in conjunction with **Authentication**. The password credential object used to authenticate to the SNMP console.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

Field	SNMP Version[1]	Description
Privacy	v3	Works in conjunction with **Authentication**. Enables or disables SNMP v3 privacy encryption.
Protocol	v3	Works in conjunction with **Privacy**. Defines the encryption protocol *AES* or *DES*. *AES* is the default.
Passphrase	v3	Works in conjunction with **Privacy**. The password credential required to authenticate to the SNMP console.

Customizing the Management Information Base

For each Simple Network Management Protocol (SNMP) channel object, you must generate and distribute the *venafi.mib* file to the SNMP management console. If you change event definitions, or if you upgrade to a new version of Trust Protection Platform, you can should and redistribute the .mib file.

To generate the file, you run the GenerateMIB utility. GenerateMIB maps events to specific Object Identifiers (OID)s in the .mib file. The OIDs include the Trust Protection Platform event fields and descriptive event text so administrators can look for specific traps in their monitoring systems.

To generate the Venafi Trust Protection Platform MIB file

1. Open Venafi Configuration Console (VCC) or the Venafi Tools MMC Snap-in.

   NOTE You must have `Read, Write` permission to the event definitions.

2. Open the **Tools** > **Logging** > **Event Definitions** node and make the desired changes.

   Now that the event definitions have changes, you need to actually generate the .mib file.

3. On the Venafi Platform server, open a command prompt.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

4. Browse to the `[drive]:\Program Files\Venafi\Platform` directory.
5. Run the `GenerateMIB.exe` utility:

   ```
   Generatemib.exe [-n:<mibname>] [-m:<modulename>] [-o:<outfile>] -c [-?|-h]
   ```

   Example:

   ```
   Generatemib.exe -n:VENAFI-MIB -m:MyCustomName -o:VENAFI-MIB.txt -c
   ```

   The `-m` switch is optional and allows you to provide a custom module name that will be displayed in your SNMP management system.

   The `-c` switch should always be used and ensures the data is refreshed from the configuration.

   This program creates the `venafi.mib` file in the current directory.

   An example of a customized MIB entry is the following:

   ```
   customizedNoCATemplate NOTIFICATION-TYPE
   OBJECTS { eventComponent, eventSeverity, eventClientIpAddressType, eventClientIpAddress,
   publicKeyFingerprint-11, certificateFolder, translatedEvent }
   STATUS current
   DESCRIPTION "Customized - No CA Template"
   ::= {director 3276817}
   ```

6. Distribute the MIB file to the SNMP management console.
7. Each time you change event definitions, re-run the `GenerateMIB` utility and redistribute the resulting `venafi.mib` file.

About syslog channels

A syslog channel allows the Venafi Log server to send log messages to any log aggregation or analyzer solution that supports the syslog protocol. Instead of a local timezone, log messages contain the GMT/UTC timestamp from the Trust Protection Platform server.

Trust Protection Platform version 19.3 introduced two new message formats–Common Event Format (CEF) and JSON–and can now support encrypted (TLS) connections to remote syslog servers. The legacy BSD format remains available.

All Venafi Log server messages include a severity code, which aligns with standard syslog severity codes. For example, 3 represents an error, 4 represents a warning, etc. Also, channel configuration settings lets administrators specify syslog facility codes.

About the CEF format

CEF, or Common Event Format, is a standardized logging format used by many network devices and applications. CEF logs contain information like the source and destination of an event, its severity, its event ID, and the message.

If the Syslog server records messages in the CEF format, the timestamps are recorded as local server time. If you are working with servers in multiple timezones, you need to be aware that per the CEF specification, dates are recorded in UTF format.

About the JSON format

If the Syslog server records messages in the JSON format, the timestamps are local time. When you select JSON as the message body format, it uses the following pattern:

```
{
  "time_stamp":"<Event.ClientTime>",
  "name":"<Event Description from Log Schema>",
  "event_id":"<Event.ID>",
  "severity":"<Event.Severity>",
  "dvc_ip":"<Event.SourceIP>",
  "object":"<Event.Component>",
  "object_id":"<Event.ComponentId>",
  "object_subsystem":"<Event.ComponentSubsystem>",
  "text1":{
    "name":<Text1 Title from Log Schema>,
    "value":<Event.Text1>
  },
  "text2":{
    "name":<Text2 Title from Log Schema>,
    "value":<Event.Text2>
  },
  "value1":{
    "name":<Value1 Title from Log Schema>,
    "value":<Event.Value1>
  },
  "value2":{
    "name":<Value2 Title from Log Schema>,
    "value":<Event.Value2>
  },
  "grouping":{
```

```
    "name":"<Grouping Title from Log Schema>",
    "value":"<Event.Grouping>"
  },
  "data":{
    "name":"<Data Title from Log Schema>",
    "value":"<Event.Data>"
  }
}
```

About the BSD format

The legacy Berkeley Software Distribution (BSD) format continues to be supported. If the Syslog server records messages in the BSD format, the timestamps are GMT/UTC time. For more information about BSD, see https://tools.ietf.org/html/rfc3164.

About TLS

Syslog channel driver can establish secure (encrypted) connection over TLS to the remote destination.

Syslog channel prerequisites

To enable the Venafi Log server to send log messages to a syslog server, ensure that you meet the following prerequisites:

- You must know the IP address or hostname of your syslog server.
- Update your firewall rules to match the port and protocol that you plan to use.

  Typically, opening firewall rules for UDP port 514 won't allow TCP traffic on that port. If you use TLS, you should select the standard port of 6514 (per RFC 5425: https://tools.ietf.org/html/rfc5425.
- Configure your syslog server to parse the message format you choose (CEF or JSON).

Syslog servers accept any message. However, if you don't configure them to parse the specific format, messages won't be captured in a way that can be consumed by Security Information and Event Management (SIEM) solutions.

To configure a syslog channel object

The Syslog Channel object stores the information that the Venafi Log server needs in order to send log messages to a syslog server.

IMPORTANT Syslog channel drivers can't recognize changes you make to either the **Allowed Outbound SSL/TLS Versions** settings or **Certificate Versions** settings. Therefore, following any changes to those settings, please restart the Venafi Log Server Windows service. For details, see "Manually stopping and starting the log server service" on page 432 in the *Log Server Administration Guide*.

To configure a syslog channel

1. In Venafi Configuration Console (VCC), navigate to **Tools** > **Logging** > **Channels**.
2. Right-click **Channels**, and then point to **Add** > **Syslog**.

   Refer to the following table while configuring your syslog channel object:

Field	Description
Host	IP address or hostname of the syslog server where you want the Venafi Log server to send log messages. The target host might look similar to one of the following examples: ◦ syslog_server.example.com ◦ 192.0.2.1 ◦ fd9d:1645:7e28:f043:6920:b203:cbe3:54ef
Format	Specify the format you want to use for your syslog messages by selecting one of the following: ◦ **BSD (Legacy)** For more information, see "About the BSD format" on page 496. ◦ **Common Event Format** (CEF) For more information, see "About the CEF format" on page 495. ◦ **JSON** For more information, see "About the JSON format" on page 495.
Facility	Facility code for the syslog channel. This option is available only if you use the BSD format. A facility code is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently. By default, the Syslog channel uses facility 16, or Local0, which is the first unassigned facility value in the list. For more information on syslog facility values, consult RFC 3164 (https://tools.ietf.org/html/rfc3164).
Protocol	Select either TCP or UDP (the default). The *user datagram protocol* (UDP) has been the most common transport layer protocol for network logging with the server listening on port 514. As UDP lacks congestion control mechanisms, TCP must be used for situations where *transport layer security* (TLS) is required.
Port	Specify the port of your syslog server.

Field	Description
	By default, the Syslog channel uses UDP port 514. To change the port number, specify it here. For example, if you want to use UDP port 1022, select the UDP protocol and type 1022 in the Target Port field.
Use TLS (Conditional)	(Conditional) If you want to establish an encrypted TLS connection to a remote syslog server, you must select TCP as the protocol and set Enable TLS to **Yes**.
Certificate	(Optional)(Conditional) If you enabled TLS, you can select a certificate credential in cases where the remote syslog server requires authentication using a specific client certificate.

3. When you're finished, click **OK**.

4

Working with notification rules

Notification rules send logging information for specific events to the defined channels.

IMPORTANT Your default log channel receives all events. Notification rules are used to send the logs of specific events to a channel other than your default channel. Do *not* send notifications to your default logging channel because this results in duplicate logged events.

This chapter contains the following topics:

Notification rule editor operators 350

Notification rule variables and supported operators 352

Login failure notification 354

Successful login from unknown IP address notification 354

Showing the correct IP address when using a load balancer to show the correct IP address 355

Venafi MMC Snap-In Collection 361

Chapter 40: Log server 418

Chapter 41: Default channel 418

Chapter 42: Event definitions for server components 419

Chapter 43: Logging tree 421

Venafi Configuration Console or the Tools MMC Snap-in? 421

Event definitions VCC Node 422

Channels VCC Node 422

Notification Rules VCC Node 423

Servers VCC Node 423

Chapter 44: Log events 424

Chapter 45: Event IDs and severity levels 424

Chapter 46: Customizing event definitions 425

Resetting to original event definitions 426

Chapter 47: Creating custom logging event definitions 426

Creating notification rules

Notification rules connect events with channels so that the event's logging information can be passed along to the specified channel.

Trust Protection Platform provides several default notification rules you can edit or use to create new notification rule objects.

Notification rules can be seen as a type of filtering tool. They contain filtering criteria that either match or don't match system events. For each system event, the log server checks each notification rule to see if its rules match the event. If it matches, the log is passed to the channel (or channels) configured for the notification rule. If the event doesn't match the notification rule, the system takes no additional action.

You use notification rules to tell the system which events are important to you, and what logging action to take when one of those events occurs. These logging actions are defined in channels.

Notification rules answer the question "What events are important?" Channels answer the question "What should happen when an important event happens?"

For example, if you want to email important events to your mailbox, you must select an SMTP channel that is configured to relay events to your email address. Similarly, if you want to log specific events to a MS SQL database, you must select a MS SQL channel that is configured to write the events to the correct database and table. You can define multiple channels for any given notification rule.

To create a notification rule:

1. In Venafi Configuration Console (VCC) or the Tools MMC Snap-in, open **Tools** > **Logging** > **Notification Rules** .

   > **NOTE** You must have `Create, Write` permission to the Notification Rules folder.

2. In the Actions panel, click **Create new notification**.

   To use an existing rule as a template, you can also choose a pre-configured rule from the **Built-In** list, then click the **Duplicate** action.

3. In the **Add Notification** dialog, specify a name for the notification rule , and then click **Add**.

4. Complete the notification rule configuration, and then click **Apply**.

The following table outlines the configuration settings for notification rules.

Field	Description
Description	A short explanation of the purpose of the rule. This will be displayed at the bottom of the Actions Panel in the Description section.
Target Channels	Channel objects the Venafi Log server uses to provide event responses or log the events. Click the Search box to load a list of channels. You can select multiple channels for any given notification rule.
Notification Disabled	Disables the current Notification Rule object.
Edit the Rule	Opens the Rule Editor. The Rule Editor is described in the following section.

Working with the Rule Editor

The Rule Editor is where you compose and test your notification rules. It has the following sections:

- **Rule Text.** This is the editor where you create your rules. While the rule is valid, you see a green check at the top of the section. When the rule is not valid, you see a red X. As you are typing, the upper-right corner of the section gives feedback on how the rule is interpreted or where it thinks there may be errors.

  Press `Ctrl + H` to see the auto-complete help window. Depending on context, the auto-complete will show what options or operators are valid. The operators are described in the table in the next section.

  You can't save the rule unless it is evaluated as being a valid rule.

- **Sample data.** Below the rule text is a series of fields where you can enter sample data. This helps you see the notification results, and helps you target your rule for specific conditions.

- **Rule Analysis.** For valid rules, it shows the order the logic is processed. This can be really helpful for complex notification rules, so you can ensure the rule text is evaluated the way you expect.

- **Processing Result.** Shows how the rule would process, based on the rule text and the sample data. If the rule and sample data combination would generate a notification, you see a green check. If the rule and sample data combination would not generate a notification, you see a red stop sign. This section then shows why it returned that result, helping you fine tune your notification rule.

- **Event Browser.** Shows all the defined system events. Click once on an event to see the sample data for that event. Double-click on an event to add that event's ID to the Rule Text.

  Use the Filter box to find specific events. The filter matches both the event category and the event name.

Notification rule editor operators

The notification rule language is human readable and writable. It supports bracketing, boolean operators, short-circuit decisions, and allows complex decisions to be expressed.

The following table shows all the operators that are supported. To see which variables can use which operators, see the next section.

Operator	Syntax[1]	Description
== (Equals)	`a == b`	Compares if `a` is equal to value `b`. Returns `true` if they are equal, otherwise returns `false`.
!= (Not Equals)	`a != b`	Compares if `a` is not equal to value `b`. Returns `true` if they are not equal, otherwise returns `false`.
IN	`a in [0010, 0020,0030]`	Checks if value `a` is present in the specified `[group]`. Returns `true` if it is, otherwise returns `false`. The group is a comma separated list inside square brackets.
IS	`a IS EMPTY`	Argument must be one of: ■ **Empty** - Null or empty string ■ **DN** - Value is DN ■ **Number** - Value is a number ■ **Letters** - Value is only letters ■ **Whitespace** - Value is only whitespace
MATCHES [2]	`MATCHES "\\\\VED\\\\Policy\\\\.*"`	Argument is a regular expression and variable must have a match to be TRUE.
LIKE	`LIKE "rest"` or `LIKE "198.51.100.14/24"`	For strings, acts as a "contains." For IP address: Argument is CIDR, and Source IP must be part of CIDR range.
<	`a < b`	Checks if value `a` is numerically less than value `b`. Returns `true` if it is, otherwise returns `false`.
>	`a > b`	Checks if value `a` is numerically greater than value `b`. Returns `true` if it is, otherwise returns `false`.

[1] String arguments should be entered with quotation marks.

[2] Regular expressions are only supported using the `MATCHES` operator, and use .NET regular expression syntax. See "Using regular expressions in a notification rule" on page 506.

Operator	Syntax[1]	Description
<=	`a <= b`	Checks if value `a` is numerically less than or equal to value `b`. Returns `true` if it is, otherwise returns `false`.
>=	`a >= b`	Checks if value `a` is numerically greater than or equal to value `b`. Returns `true` if it is, otherwise returns `false`.
&&	`a && b`	Logical AND. Returns `true` if both `a` and `b` are `true`. Otherwise, returns `false`.
||	`a || b`	Logical OR. Returns `true` if either `a` or `b` is `true`. Otherwise, returns `false`.
!	`!a`	Logical NOT. Inverts the value of `a`. Returns `true` if `a` is `false`, and `false` if `a` is `true`.

Notification rule variables and supported operators

The following table shows the supported variables, and what operations are allowed for each variable.

		Rules					
Variable	Example	== !=	< <= > >=	LIKE	MATCHES	IS	IN
Component	`\VED\Policy\Abc`	✓		✓	✓	✓	✓
Data[2]	`Some Text`			✓	✓	✓	✓
EventID	`0x001f0003`	✓	✓				
Grouping	`154`	✓	✓				✓
Severity	`Info`	✓	✓				✓
SourceIP[3]	`192.168.3.4/24`	✓		✓			✓
Text1	`Some Text`	✓		✓	✓	✓	✓
Text2	`Other text`	✓		✓	✓	✓	✓
Value1	`123`	✓	✓				✓
Value2	`456`	✓	✓				✓

[1] String arguments should be entered with quotation marks.

[2] Data is assumed to be encoded UTF-8 text and converted to UTF-8 before operators are applied.

[3] SourceIP supports both IPv4 and IPv6 addresses and CIDR notation.

Using regular expressions in a notification rule

Regular expressions allow you to search for patterns of data such as email addresses or IP addresses. In Venafi Trust Protection Platform, regular expressions are used in Notification Rules to search for patterns of data using the `MATCHES` operator. In Venafi Platform, RegEx follows the .NET Framework syntax.

For example, the following regular expression searches for an Internet email address:

```
\b[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}\b
```

If the event data in the designated field matches the pattern specified in the regular expression—i.e., an Internet email address—the event triggers the Notification Rule and a notification is sent via the designated target channels.

For more information on regular expressions, see:

.NET Framework Regular Expressions (http://msdn.microsoft.com/en-us/library/hs600312.aspx)

and

Regular Expression Language Elements (http://msdn.microsoft.com/en-us/library/az24scfc.aspx).

Configuring expiration event intervals

You can define the intervals at which Trust Protection Platform generates expiration events for certificates, symmetric keys, and SSH keys at the object level in individual Certificate, SSH key, or Symmetric Key objects; or you can manage the expiration event intervals via policy.

The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in notification and channel objects. By default, Trust Protection Platform provides default notification rules for expiration events. You can see these rules in Venafi Configuration Console (VCC), or in the Tools MMC Snap-in collection.

Configuring your system for login notifications

Venafi Platform ships with two default email notifications for login security. These notifications help secure your environment by alerting users to successful login attempts from unknown IP addresses, as well as all unsuccessful login attempts. These notifications are enabled by default.

Each of these notifications is described below, followed by important configuration information if you are using a load balancer.

Login failure notification

It is important that users be alerted any time an attempt to log in fails in case somebody is trying to break into their account. This notification will trigger anytime a user attempts to log in to Venafi Platform but the login attempt fails. This may be due to an incorrect password, or another authentication issue.

This notification goes to the user whose login was used in the login attempt, and includes the IP address of the user attempting to log in.

The notification rule in VCC is called **Login Failure**, and is in the Built-In folder.

The target channel is called **Email to Owner - Login Failure**.

The subject of the email is "Account Login Failure".

Successful login from unknown IP address notification

Sometimes you want users to be notified anytime a login happens from an unknown IP address. This notification triggers anytime a user successfully logs in to Venafi Platform from an unknown location (as determined by IP address). This notification goes to the user who successfully logged in, and includes information about the login, including the IP address of the user who successfully logged in. This notification is important because it helps users monitor logins from remote locations. If a user doesn't recognize a location, their account information may be compromised.

IP history is stored with each user's preferences, so if users clear their preferences (**User menu** > **My Account** > **Reset Settings & Preferences**), their location history will also be reset.

The notification rule in VCC is called **Login Successful from Unknown Source**, and is in the Built-in folder.

The target channel is called **Email to Owner - Login Successful**.

The subject of the email is "Account Login from New IP Address".

Showing the correct IP address when using a load balancer to show the correct IP address

If you are using a load balancer, you need to configure the load balancer to log the `X-Forwarded-For` header. If the load balancer is not configured correctly, these notification will show the IP address of the load balancer. This is especially important for the successful login notification, because without the `X-Forwarded-For` header on the load balancer, the notification is essentially meaningless, since *all requests* will appear to be coming from the load balancer.

Logging the `X-Forwarded-For` header provides better security logs for web activity that comes through a load balancer, and will help you troubleshoot your load balancer. (If you are not sure if your load balancer is properly configured to send the `X-Forwarded-For` header, you can check your IIS logs on your Venafi server.)

This is done in two steps: 1. Configure your load balancer to pass the client IP address in the `X-Forwarded-For` header; and 2. Configure your Venafi server IIS settings to log the `X-Forwarded-For` header.

To configure your load balancer

- Check your load balancer vendor documentation for specific steps on configuring the `X-Forwarded-For` header.

You can read reference information about the `X-Forwarded-For` header on MDN Web Docs.

To configure your Venafi server's IIS settings to log the `X-Forwarded-For` header

1. Connect to your remote Venafi server, and open Internet Information Services (IIS) Manager.
2. In the **Connections** panel, expand **Sites**, and click **Venafi**.
3. In the IIS group, double-click **Logging**.
4. Under the Log File section, click the **Select Fields** button next to the Format: W3C dropdown.
5. Click **Add Field...**
6. Set the following values:

Field	Value
Field Name	X-FORWARDED-FOR
Source Type	Request Header
Source	X-FORWARDED-FOR

7. Click **OK** to close the Edit Custom Field window.
8. Click **OK** to close the W3C Logging Fields window.
9. Restart IIS to ensure settings take effect.

When IIS restarts, the correct IP addresses will appear in the login notification email messages for all users in your organization, and will be logged on the Venafi server.

Automatic credential rotation options

Trust Protection Platform provides the ability to rotate important system credentials using user-provided scripts via a command line interface (CLI). This means if you have an external system that rotates these credentials, you can write a script that will automatically change the connection information for Trust Protection Platform automatically.

Credentials you can script for rotation:

- HSM connection pin
- Trust Protection Platform database connection password
- Identity provider. For more information, see "Updating an identity provider connection password" on page 748.

To reset the HSM connection pin using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-hsmpin` switch. For example:

```
TppConfiguration.exe -hsmpin:<pin>
```

NOTE If you don't include the PIN, the system will prompt you for the PIN in the next step.

IMPORTANT The command line process does not validate the HSM PIN or database connection string. If you provide invalid data, you will not get a warning message. If you want to validate the data, use the Venafi Configuration Console interface, which does validate both the HSM pin and the database connection string.

NOTE This utility is not designed to move your Venafi server from one database to another. It is intended only for changing credentials and scripting credential changes.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

For more information on using the command line to perform actions in Trust Protection Platform, see Configure the product from the command line in the Installation and Upgrade Guide.

To reset the Trust Protection Platform database owner account connection password using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-dboconfig` switch. The format is:

   ```
   TppConfiguration.exe "-dboconfig:<cfg>"
   ```

   For example:

   ```
   TppConfiguration.exe -dboconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOwnerUser;Password=S0me\"thing-Complex!"
   ```

   To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

To reset the Trust Protection Platform operational database account connection password using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-sqlconfig` switch. The format is:

   ```
   TppConfiguration.exe "-sqlconfig:<cfg>"
   ```

   For example:

   ```
   TppConfiguration.exe -sqlconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOperationUser;Password=S0me\"thing-Complex!"
   ```

   To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

For more information about the TPPConfiguration utility, see "Using the TppConfiguration command line tool" on page 511.

Database Connection Repair

If the database can't be accessed when trying to run Venafi Configuration Console, the Database Connection Repair wizard will be shown.

If the database server is experiencing temporary downtime, Trust Protection Platform will resume working correctly when connectivity is restored. However, if the database connection information changes, you will need to repair the database connection.

To repair the database connection

1. On the application sever, open the **Venafi Configuration Console**.

   If the Configuration Console opens, the application server was able to communicate with the database, and you do not need to continue.

   If the application server was not able to communicate with the database, the Database Connection Repair wizard opens.

2. Read the information in the Database Connection Repair window, then click **Next**.

3. Update the database connection information, then click **Finish**.

   - If the application server was able to connect using the updated information, the wizard will show that installation is complete, and you can click **Close**.
   - If the application server was not able to connect using the updated information, the wizard will show a connection error. Correct any errors in the database settings, and click **Finish**.

To repair the database connection from the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-dboconfig` switch. The format is:

   ```
   TppConfiguration.exe "-dboconfig:<cfg>"
   ```

For example:

```
TppConfiguration.exe -dboconfig:"Data Source=192.168.1.1,1433;Initial Catalog=databasename;User ID=dbOwnerUser;Password=S0me\"thing-Complex!"
```

To obtain your current SQL configuration string, see "Obtaining the SQL database connection string" on page 59 in the Administration Guide.

3. Restart the Venafi Windows services.
4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

IMPORTANT The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it into the connection string as `pas\"sw\\ord`.

To learn more about the TPPConfiguration utility, see "Using the TppConfiguration command line tool" on page 511.

How to recover a broken HSM connection

If your connection between Trust Protection Platform and your HSM is broken or corrupted, you will need to use the following steps to reconnect, or reconfigure the connection between the two.

You can do this either in the Venafi Configuration Console or using the command line.

To reconfigure the connection between Trust Protection Platform and an HSM using Venafi Configuration Console

1. On the Venafi server, open the Venafi Configuration Console.

   When the console loads, it will display an error message, saying the connection to the HSM failed to initialize.

   IMPORTANT When the console opens, only use the console to reconnect the HSM. Do not attempt to use the console to perform other functions until the connection to the HSM has been restored.

2. Complete the steps to create an HSM connector. For more information, see "Creating a HSM connector" on page 562 in the Administration Guide.

To reconfigure the connection between Trust Protection Platform and an HSM using the command line

1. On the Venafi server, open a command prompt and browse to the `Venafi\Platform` directory.

   If you installed Trust Protection Platform in the default directory, you would browse to the following location:

   ```
   c:\Program Files\Venafi\Platform
   ```

2. Run the configuration utility (`TppConfiguration.exe`) with the `-hsmpin` switch. For example:

   ```
   TppConfiguration.exe -hsmpin:<pin>
   ```

   NOTE If you don't include the PIN, the system will prompt you for the PIN in the next step.

   IMPORTANT The command line process does not validate the HSM PIN or database connection string. If you provide invalid data, you will not get a warning message. If you want to validate the data, use the Venafi Configuration Console interface, which does validate both the HSM pin and the database connection string.

   NOTE This utility is not designed to move your Venafi server from one database to another. It is intended only for changing credentials and scripting credential changes.

3. Restart the Venafi Windows services.

4. Restart the Venafi IIS Application Pools, or perform an IIS Reset.

For more information on using the command line to perform actions in Trust Protection Platform, see Configure the product from the command line in the Installation and Upgrade Guide.

Venafi MMC Snap-In Collection

The Venafi MMC Snap-In Collection includes snap-ins that can be installed on a standalone Windows workstation, so you don't have to be logged on to the Trust Protection Platform server to use them. The following Snap-Ins are included:

- **Venafi Access Management**

  Allows authorized users to manage API applications from a remote Windows device.

- **Venafi CodeSign Protect Administration**

  Allows Code Signing Administrators to perform code signing administrative tasks without having to sign in to the Trust Protection Platform server.

- **Venafi Event Viewer**

  Provides detailed views in Trust Protection Platform events from the event logs.

- **Venafi Statistics Viewer**

  Provides extensive Trust Protection Platform statistics.

- **Venafi Recycle Bin**

  Allows administrators to configure automatic pruning of outdated database information, and allows administrators to revert some deletions by users.

- **Message Bus**

  Allows administrators to view the status of the message bus and identify and troubleshoot potential network connectivity issues across all servers in the cluster.

- **Tools**

  Provides the ability to interact with additional tools for managing your system. Currently, the only tool that is included is Logging, but future tools will be added to this node.

  - **Logging** - Released in 25.1, the Logging node replaces the Logging tree in the now-deprecated WinAdmin console. The Logging node allows you to customize all logging and notification settings for your environment including modifying e-mail templates and SMTP notification settings.

DID YOU KNOW? You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.

Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

This chapter contains the following topics:

Install the Venafi MMC Snap-In Collection

> **NOTE** This procedure provides instructions on installing the Venafi MMC Snap-In Collection. The snap-in collection can be installed on any Windows workstation, thereby allowing administrators to perform management tasks without having to be signed in to the Trust Protection Platform server.

In order to complete this procedure, you'll need the following information:

- URL of the Trust Protection Platform SDK endpoint

  If the default engine settings are used, this is: `https://[venafi-server]/vedsdk/`

- URL of the Trust Protection Platform authentication endpoint

  If the default engine settings are used, this is: `https://[venafi-server]/vedauth/`

- Valid user credentials to the Trust Protection Platform server and access to use the snap-ins.

  While users may have access to view the snap-in, they must also have rights to see the data. For example, the Venafi Recycle Bin snap-in can be added by anybody, but the contents of the recycle bin can only be seen by a master administrator.

- API access granted to the user.

  The snap-in collection utilizes Venafi's API, so to use the snap-ins, your user account needs API access. This is covered in the next section.

- Authentication method information.

  You can log in using your Venafi user name and password, or you can use Windows Integrated Authentication (if itself has been configured to use Windows Authentication). Please review the following topics for information on configuring to use Windows Integrated Authentication:

  - "Setting up Windows Integrated Authentication for the web console" on page 797
  - Setting up Integrated Windows Authentication for API access

The Snap-In Collection requires the following:

- .NET 4.7.2
- Windows 8.1 or later **or** Windows Server 2016 or later

Grant access to the snap-ins

In order to use the MMC snap-ins, a master admin must grant access to them. The relevant Application Names for the snap-ins in the MMC snap-in collection are:

- Venafi Code Signing Administration
- Venafi Configuration Console
- Venafi Event Viewer
- Venafi Statistics Viewer
- Venafi Recycle Bin
- Venafi Access Management
- Venafi Message Bus
- Venafi Tools

To use the any of the MMC snap-ins, users must be given access by an administrator. To grant access, use the **Integrations** page in the **Platform** product.

1. Sign in to the Venafi Platform product, and click **API** > **Integrations** in the menu bar.

   > **TIP** Use the filter to search for `MMC` to see all the snap-ins.

2. Click the name of the snap-in you're granting access to.
3. Click **User or team access**.
4. In the **User or team** box, enter the name of the user or team you want to grant access to.
5. Click **Add**.
6. Click **Save**.

Once users have access, they can install and configure the snap-in.

After access is granted to use the snap-ins, return to this topic and follow the steps below to load them in the MMC.

Download and install the Venafi MMC Snap-In Collection

1. Download the **VenafiMmc-25.1.0.msi** installation file. See download.venafi.com.
2. Run the installation file. The **Venafi MMC Snap-In Collection Setup** wizard opens. Click **Next**.
3. Accept the end-user license agreement and click **Next**.
4. Select the location where you want the Venafi MMC snap-in installed. Click **Next**.
5. Click **Install**. The installation takes place. Click **Finish**.

Add the Snap-Ins to the MMC

> **DID YOU KNOW?** You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.
>
> Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

1. On the Windows computer where you want to run the snap-in, open the MMC console.

   You can do this by pressing **Windows+R** and typing mmc in the **Open** box. Click **OK**, and then click **Yes** in the User Account Control window.

2. Click **File** > **Add/Remove Snap-In**.
3. From the **Available snap-ins** list, locate the Venafi snap-ins. They all start with the word *Venafi*. For each snap-in that you want to add, follow the instructions below:

Venafi CodeSign Protect Administration

You must have a valid access grant to use the Venafi CodeSign Protect Administration snap-in prior to completing these steps. See "Grant access to the snap-ins" on the previous page.

Select the Venafi CodeSign Protect Administration snap-in, and then click **Add**.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.
  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Click **OK**.The snap-in is added to the **Selected snap-ins** list.

Venafi Event Viewer

You must have a valid access grant to use the Venafi Event Viewer snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Event Viewer snap-in, and then click **Add**.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.

  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Click **Connect**. After connecting, you will see **Channel** and **Result Limit**.

The **Channel** drop-down shows all configured SQL channels that log event data. Select the one you would like to view data from.

The **Result Limit** drop-down is the default limit that will be used for any retrieved records, if a custom view does not specify a limit. For example, if you select 50,000 and a query has more than 50,000 results, only the 50,000 newest events will be returned and displayed.

Click **OK**.The snap-in is added to the **Selected snap-ins** list.

Venafi Statistics Viewer

You must have a valid access grant to use the Venafi Statistics Viewer snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Statistics Viewer snap-in, and then click **Add**.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.

  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Click **OK**.The snap-in is added to the **Selected snap-ins** list.

Venafi Configuration Console

You must have a valid access grant to use the Venafi Configuration Console snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Configuration Console snap-in, and then click **Add**.

Please note that users must have the Master Admin role to see the contents of the Venafi Configuration Console snap-in.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.
  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Remember, you will only see content in this node if you have the Master Admin role.

Click **OK**.The Venafi Configuration Console snap-in is added to the **Selected snap-ins** list.

Venafi Recycle Bin

You must have a valid access grant to use the Venafi Recycle Bin snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Recycle Bin snap-in, and then click **Add**.

Please note that users must have the Master Admin role or the Recycle Bin Admin role to see the contents of the Recycle Bin snap-in.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.
  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Remember, you will only see content in this node if you have the Master Admin role or the Recycle Bin Admin role.

Click **OK**.The Venafi Recycle Bin snap-in is added to the **Selected snap-ins** list.

Venafi Access Management

You must have a valid access grant to use the Venafi Access Management snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Access Management snap-in, and then click **Add**.

Please note that users must have the Master Admin role to see the contents of the Venafi Access Management snap-in.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.

  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Remember, you will only see content in this node if you have the Master Admin role.

Click **OK**.The Venafi Access Management snap-in is added to the **Selected snap-ins** list.

Venafi Message Bus

You must have a valid access grant to use the Venafi Bus Management snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Bus Management snap-in, and then click **Add**.

Please note that users must have the Master Admin role or the Recycle Bin Admin role to see the contents of the Recycle Bin snap-in.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.

  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Remember, you will only see content in this node if you have the Master Admin role or the Recycle Bin Admin role.

Click **OK**.The Message Bus snap-in is added to the **Selected snap-ins** list.

Venafi Tools

You must have a valid access grant to use the Venafi Tools snap-in prior to completing these steps. See "Grant access to the snap-ins" on page 364.

Select the Venafi Tools snap-in, and then click **Add**.

Please note that users must have the Master Admin role to see the contents of the Venafi Tools snap-in.

In the **Venafi Selection** dialog, enter the following:

- **Title**: Enter a title for this connection.

  This will be used as the root node of the snap-in. Since you can have more than one Venafi Platform instance, you should give it something that helps you know which Venafi Platform this item is connected to.

- **Host URL**: URL of the Trust Protection Platform SDK server.

  If you haven't modified the engine's default settings, the format is https://[venafi-server]/vedsdk/.

- **Auth URL**: URL of the authentication Trust Protection Platform server.

  If you haven't modified the engine's default settings, the format is: https://[venafi-server]/vedauth/.

  Correct format is https://[server URL]/vedauth/.

- **Method**: Select the method of authentication.

  - Select **Credentials** if you want to log in with the user name and password you use to access Venafi Platform.

  - Select **Integrated Authentication** if you want to use Windows Authentication.

- **Username** and **Password**: If you are using the *Credential* method, enter the user name and password you use to access Venafi Platform. If you are using the *Integrated Authentication* method, these fields are disabled.

Remember, you will only see content in this node if you have the Master Admin role.

Click **OK**.The Venafi Tools snap-in is added to the **Selected snap-ins** list.

4. Click **OK**.

Saving the Snap-In view

Once the snap-in is loaded, you can save your view for quicker access in the future. In the MMC, click **File** > **Save**. Choose a name and location for your .msc file, and click **Save**. Double-clicking the .msc file opens the MMC with the snap-in already loaded.

Venafi CodeSign Protect Administration Snap-In

For detailed information about the Venafi CodeSign Protect Administration MMC Snap-In, see "Code Signing" on page 170.

Venafi Event Viewer

The Event Viewer snap-in supports viewing multiple Event Logs simultaneously by being added multiple times to the same MMC workspace.

> **DID YOU KNOW?** The Venafi Event Viewer node can be run as an MMC Snap-in on standalone Windows workstations. For more information, see "Venafi MMC Snap-In Collection" on page 361.

Some notable features include:

- Summary view providing event statistics
- All events view providing events of the last 7 days
- Support for named custom views
- Custom views allow to select displayed events by application, event, time frame and severity
- To allow fast retrieval, the number of events in a view can be restricted to a configurable number of returned events, newest first
- Custom views are saved as Trust Protection Platform preference of the user

This chapter contains the following topics:

Venafi Event Viewer overview

Log Summary

The Log Summary summarizes all events of the last 7 days. It also breaks down which events occurred in the last hour and in the last 24 hours. The events are grouped by **Event Type** (Severity).

The data for the tab is loaded once the node is first selected. While the data is being loaded, progress information is displayed in the top section of the view. The data will stay loaded even if another node is selected before returning to the summary view. To update the data, click **Refresh** from the Actions Panel.

To see which event occurred, expand one or more Event Type nodes by clicking on the  icon. Each event will have the name (**Event ID**), and it's source (**Application**) displayed, along with a count for the **Last Hour**, **24 hours**, and **7 days**.

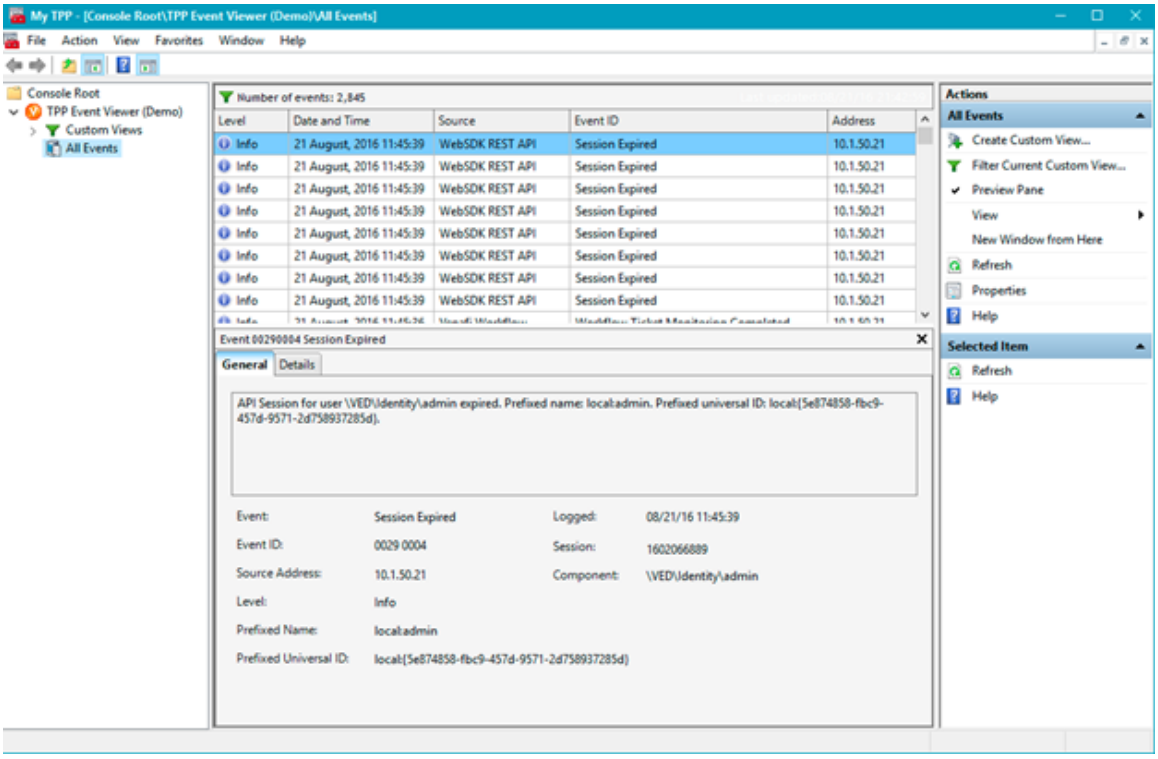
Right-clicking a column header gives you options on how to present the data.

Summary of Events

The summary of events presents all events present in the log by count and as percentage of all events. Right-clicking a column header gives you options on how to present the data.

All Events

The **All Events** node is always present and cannot be deleted. It displays the events of the last 7 days, subject to any configured limit of rows. To open this view, click **All Events** in the left panel.



Event detail nodes always provide a list of events in the upper pane, and a Preview Pane in the bottom section. The Preview Pane can be turned off by unchecking **Preview Pane** in the Actions Panel.

The Preview Pane displays event details. The “General” tab in the preview pane has a text area that contains the translated event. Below the text area each field present in the event is listed explicitly, with both field name and it’s value.

The **Details** tab shows the raw event data.

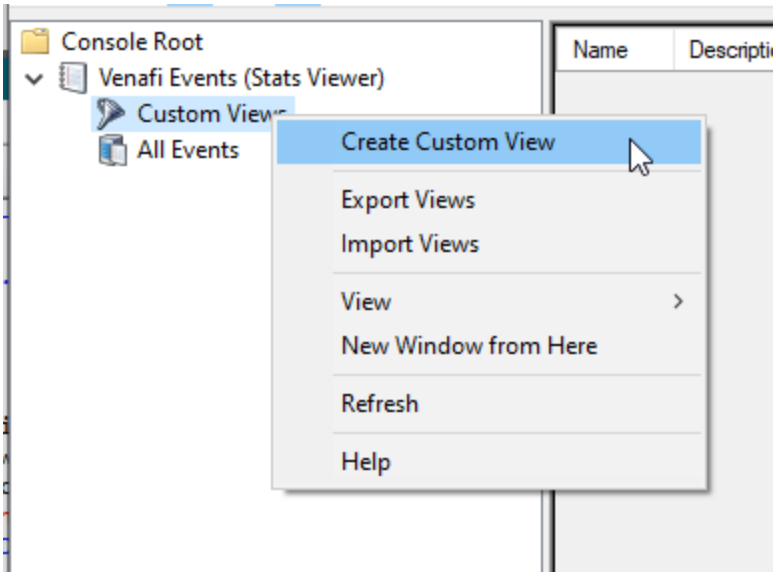
Custom Views

The Event Viewer snap-in allows you to create, save, and share custom views. All created custom views are automatically saved under the Trust Protection Platform user’s preferences on the Trust Protection Platform server associated with the query.

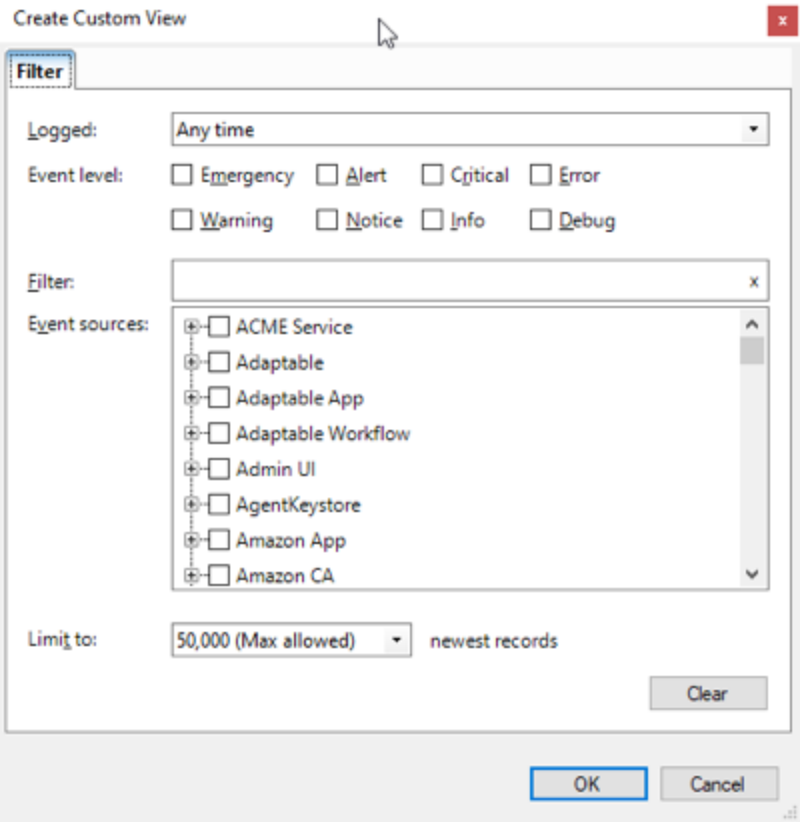
Create a new Custom View

To create a new Custom View, click **Create Custom View** from the Action Panel on any Event Detail View (or right-click an **Event Detail** node).

NOTE Saved views are saved to your Trust Protection Platform user preferences. As such, saved views are available on *any* system where you use the snap-in against the same Trust Protection Platform server using the same user credentials.



The snap-in will display the **Create Custom View** dialog, which allows you to select the timeframe or age of events, the Event level (Severity), as well as the applications and specific Event IDs.

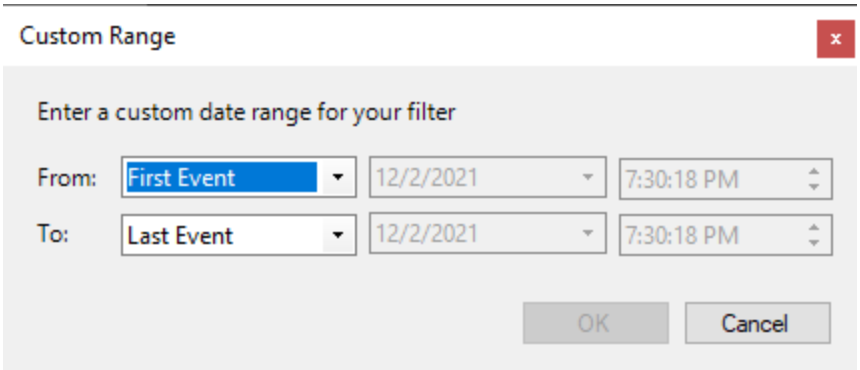


Select timeframe

From the **Logged** drop-down, select a timeframe for this view.

To chose a specific date range, select **Custom range**, and the snap-in will display the **Custom Range** dialog, allowing you to narrow the range.

First Event represents the oldest event. **Last Event** represents the newest event. To pick a specific start or end date, select **Event On** from either drop-down.



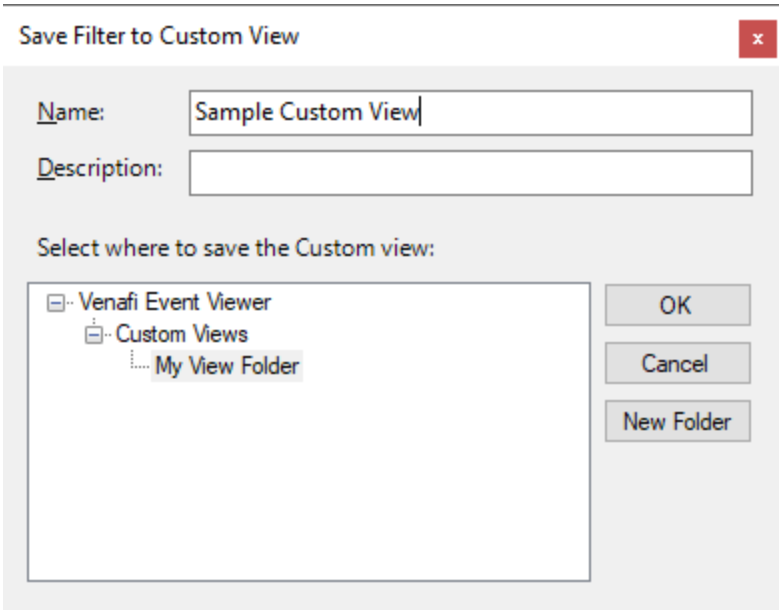
Select filter criteria

Select one or more of the **Event levels**. Then, use the **Event sources** box to select the events that you want to include.

> **TIP** Use the **Filter** field to quickly search the event sources options. Start typing the name of any event source, and the list will filter based on your entry.

Save the custom view

After choosing your filter criteria, click **OK** to get the **Save Filter to Custom View** dialog. In this dialog, you can provide a name and description for your new view, and you can create and choose what folder to save your view under.



For **OK** to be enabled, at a minimum you must provide a name and select a folder. In this example, we used the **New Folder** button to create the **My View Folder** to save the new view under.

Once saved, the new view is immediately loaded and displayed.

Edit an existing Custom View

To make changes to an existing view, select the view node and click **Filter Current Custom View** in the Actions Panel.

Save and open event logs

To save a current log, click **Save Events Log As** in the Actions panel. This exports the current log in CSV format.

To open a previously-saved log, click **Open Saved Log** and select the log you want to import.

Import and export views

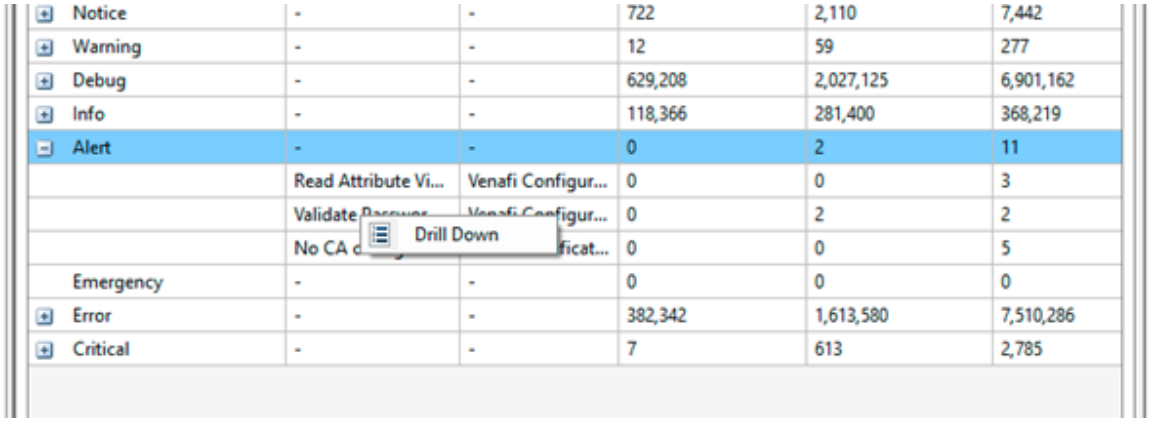
To export your current view to a JSON file, select a folder (not a saved custom view) in the navigation panel. Then, in the Actions panel, click **Export Views**. From here, you can select what views you want to export.

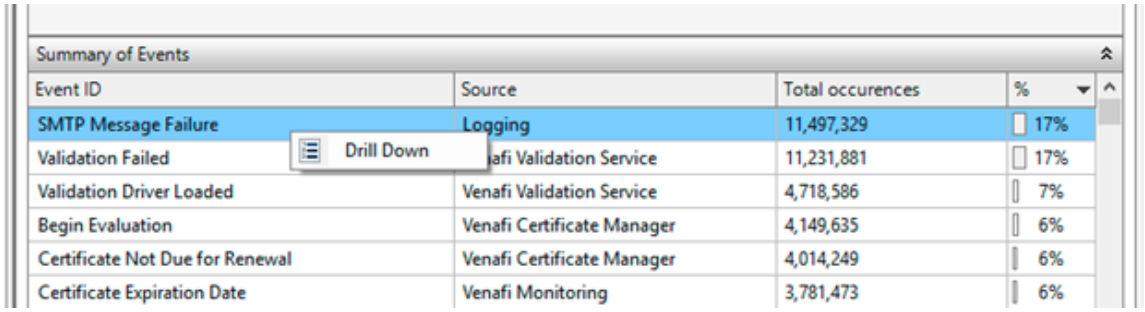
> **TIP** The **Export Views** feature is best used for sharing views with other users, or for copying views from one environment to another (such as from dev to production).
>
> Saved views are automatically available from any machine where you add the snap-in against the same Trust Protection Platform server using your same credentials.

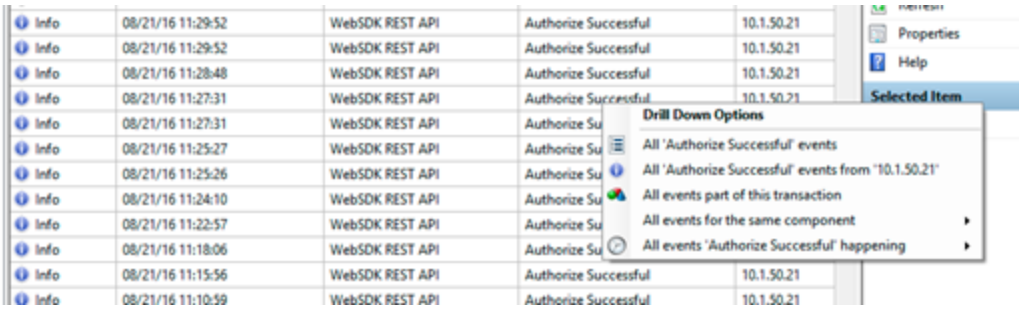
The JSON file that is saved when a view is exported can subsequently be imported on another machine. Click on a folder in the navigation panel, and then click **Import Views**, and select the previously-exported JSON file.

Drill down queries

The Snap-in has the ability to generate automatic drill-down queries. The **Event ID** cells on the **Summary** and **Overview** nodes, as well as all cells in an event list allow to right-click and get a drill-down option menu:

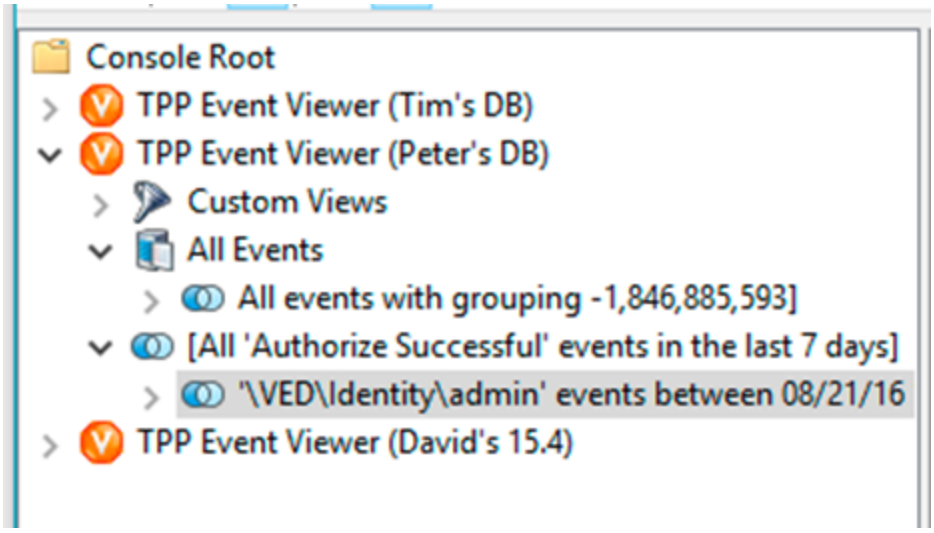


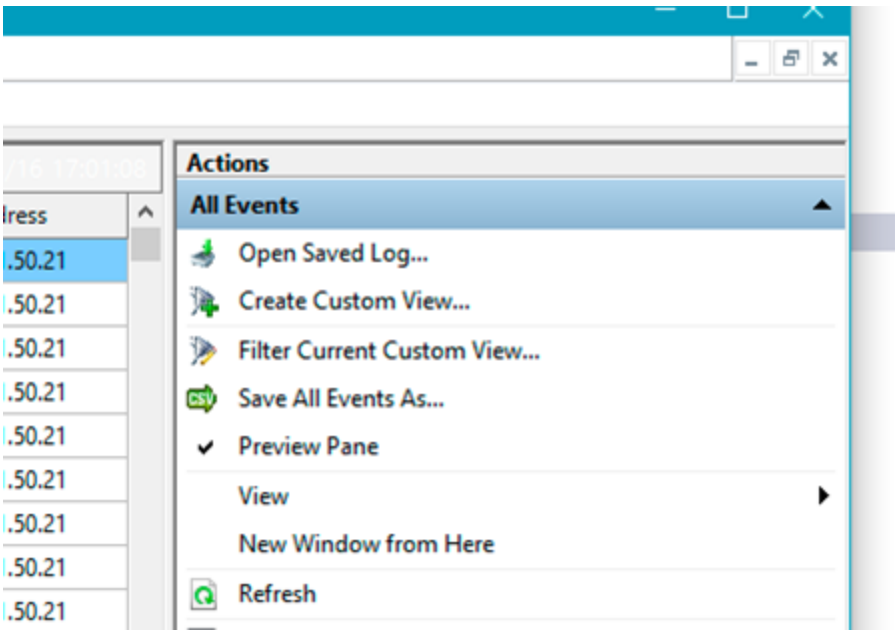




A drill-down selection creates a special node, indicated by the  icon for the node. Drill-down nodes are temporary and not saved. A drill-down node is always created as a child of the view the drill-down was initiated from.

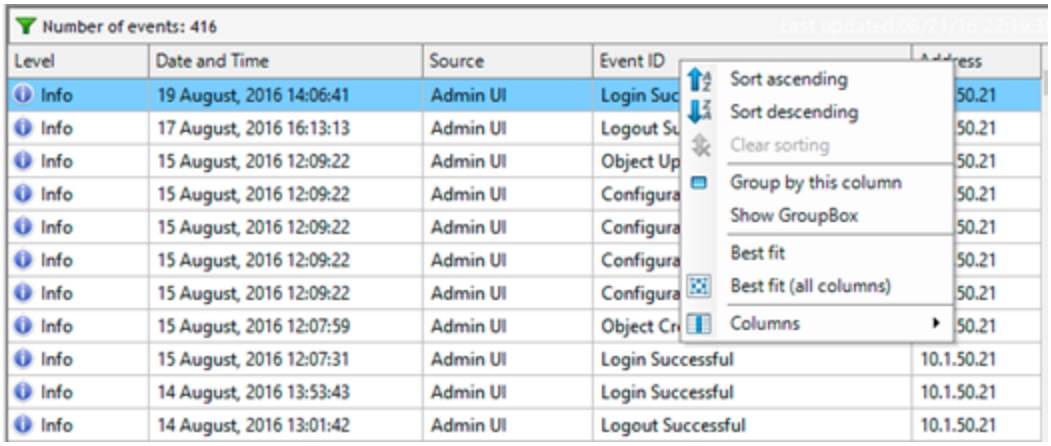
On the event list view, drill-downs are context sensitive to both the column selected, and the underlying data of the event. For example, if an event has a grouping (transaction) indicator, the option to see all events of the transaction will be available. Using a drill-down is a fast way to see related events.



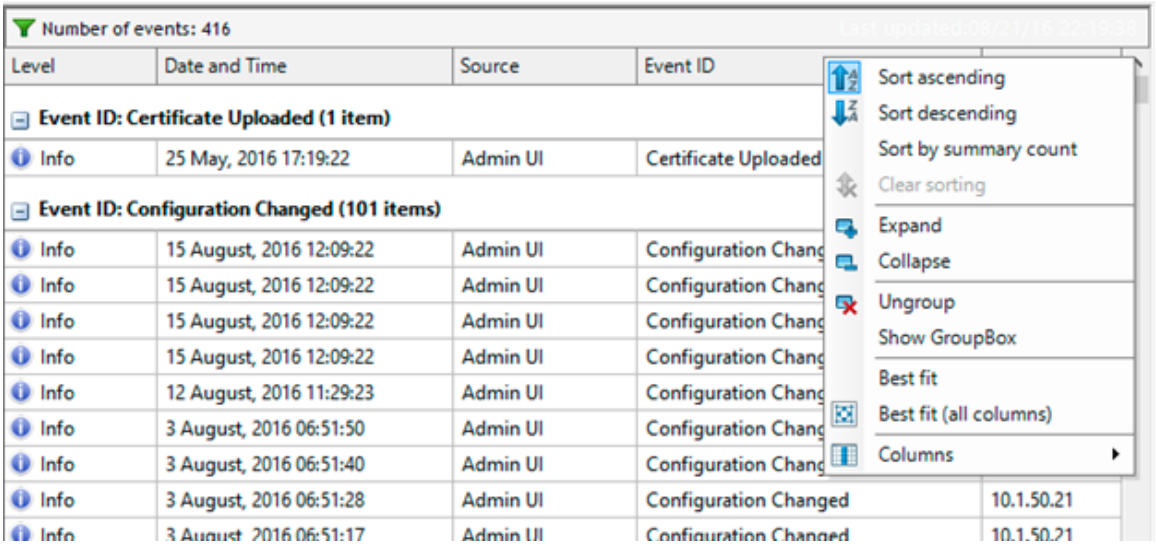


Organize the event list

The Event List grid, much like the Summary grids, allows you to group and organize the displayed events. To group by a particular column, right-click the column and select **Group by this column**.



Once grouped, right-clicking on the grouped column allows to collapse all groupings by selecting **Collapse**.



This will give an overview, with count, of all unique items in the grouped column.

To drill down and understand the events better, other columns can be added to the grouping, by repeating the above steps with one or more columns.

Saving the configuration

To save the configured Snap-in configuration and layout, click **File** > **Save** in the MMC, and pick a name for your configuration.

To re-open MMC with that configuration later, simply double-click the saved file or run it from **Start** > **Run** or the Windows Search Bar.

The Trust Protection Platform configuration and the authentication token reference is saved in the .MSC file. Passwords will not be saved. When a saved MSC file is opened and the access token is expired, the Snap-in will prompt for the username and password, displaying the title and URL for context.

Import and Export of events

The Snap-in allows to export the data of a view to a CSV file. This allows to provide events to Support for analysis. To save data, select **Save All Events As** from the Action Panel.

To load a saved event CSV, select **Open Saved Log** from the Action Panel.

Imported events will placed into a child node of the currently selected node.

Venafi Statistics Viewer

The Venafi Statistics Viewer snap-in allows you to view detailed statistics about your Trust Protection Platform server's activity and performance.

> **DID YOU KNOW?** The Venafi Statistics Viewer is also available as a node in the Venafi Configuration Console (VCC). Whereas the VCC requires you to be logged in to the Trust Protection Platform server, the MMC snap-in can be run from any Windows machine.
>
> The content in this topic applies to both the VCC node and the MMC snap-in.

Granting access to the Venafi Statistics Viewer Snap-In

To use the Venafi Statistics Viewer, users must be given access by an administrator.

1. Sign in to the Venafi Platform product, and click **API** > **Integrations** in the menu bar.
2. Click **Venafi Statistics Viewer**.
3. Click **User or team access**.
4. In the **User or team** box, enter the name of the user or team you want to grant access to.
5. Click **Add**.
6. Click **Save**.

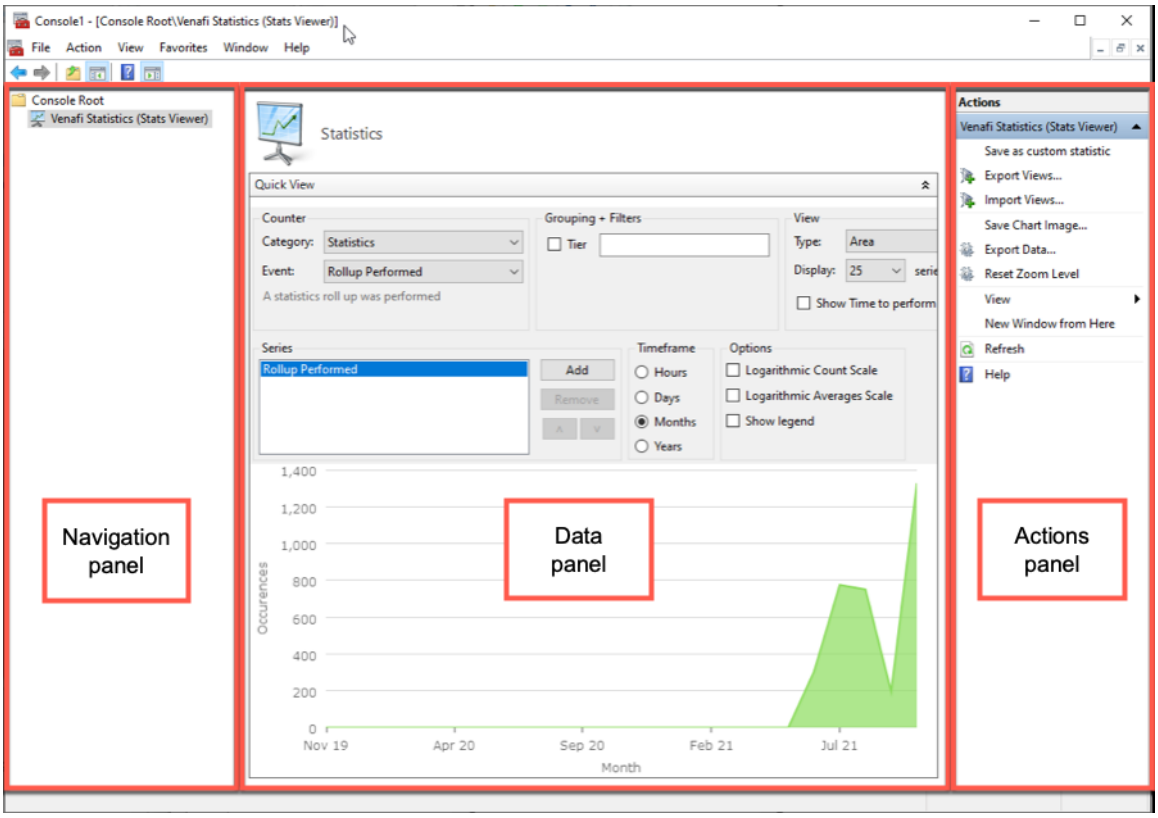
Once users have access, they can install and configure the snap-in.

Installing the Venafi Statistics Viewer Snap-In

The Venafi Statistics Viewer is included as part of the Venafi MMC Snap-In Collection. For installation instructions, see "Install the Venafi MMC Snap-In Collection" on page 363.

> **NOTE** If you're using the Statistics node in VCC, no installation is needed. Just open VCC and click the Statistics node.

Using the Venafi Statistics Viewer Snap-In



Viewing statistics

To view statistics, click **Venafi Statistics** in the navigation panel. In the data panel, the **Statistics** interface opens.

The top of the data panel provides various statistics options to select from, and the associated data will be displayed in the graph area at the bottom of the panel.

In the **Counter** box, use the **Category** and **Event** drop-downs to select what statistics to view. You can further refine the statistics report by using the options in the **Grouping + Filters**, **View**, **Timeframe**, and **Options** sections.

> **TIP** Hovering over the graph shows specific values behind the graph elements.
>
> Clicking and dragging on the graph expands the highlighted selection. This is useful to get a more granular view of the graph data. To zoom out, click **Reset Zoom Level** in the Actions panel.

Overlaying multiple statistics graphs

The **Series** box allows you to select multiple statistics and overlay them in the graph area. To add additional statistics to your current view, click **Add**. This adds an additional series, independent from all other series already defined. You can now select the statistics that you want this series to show.

The order of the series determines how the various graphs get stacked in the graph area. You can adjust the order using the up and down arrow buttons.

Example

In this example, we'll view the total number of successful code signing operations *and* the average time to sign on the same graph.

First, from the Counter drop-downs, select the **Code Signing** category and the **Signing Successful** event. In the View box, select **Column** for the type, and from the Timeframe box, select **Months**. The graph now shows a bar graph with the total number of successful signing operations per month.

Next, click **Add** in the Series box. This adds a new series.

For this series, select **Code Signing** and **Signing Successful** again from the Counter drop-downs. Then, in the View box, click the **Show Time to sign** checkbox. A line with the average signing time per month is overlayed on top of the chart.

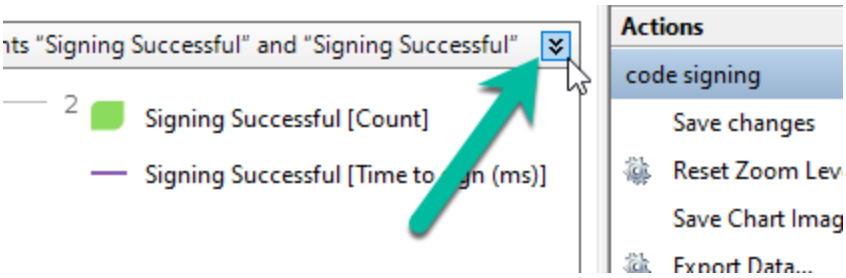
Saving a statistics view

To save a particular statistics view, click **Save as custom statistic** in the Actions panel on the right. Then provide a name and location to save your view. Once saved, the view is available in the left navigation panel.

NOTE Saved views are saved to your Trust Protection Platform user preferences. As such, saved views are available on *any* system where you use the snap-in against the same Trust Protection Platform server using the same user credentials.

Editing a saved statistics view

To edit a saved view, open the view from the navigation panel. If the statistic selections aren't showing at the top of the data panel, click the expand icon in the top right corner of the data panel.



After making changes, click **Save changes** in the Actions panel.

Options available from the Actions panel

Option	Description
Save as custom statistic	Saves the current statistics view to the user's Trust Protection Platform profile. It is available from the navigation panel. After saving, this view is available from any machine where the snap-in is added against the same Trust Protection Platform server using the same credentials. This option shows only for views that haven't previously been saved.
Save changes	Saves any changes to a previously-saved view.
Export Views	Exports view parameters to a JSON file. This file can then be imported using the **Import Views** action on another machine.

Option	Description
	TIP This feature is best used for sharing views with other users, or for copying views from one environment to another (such as from dev to production). If you just want to make this same view available to yourself from another machine, use the **Save as custom statistic** action instead (see above for details).
Import Views	Imports JSON files that were created using the **Export Views** action. During import, you can select where you want this view saved in the navigation panel.
Save Chart Image	Saves an image of the current graph as a PNG file. Selecting the **Show legend** checkbox includes a graph legend as part of the image file.
Export Data	Exports the data to a CSV file.
Reset Zoom Level	Resets the zoom level back to the default if you've zoomed in on the graph. You can zoom in by clicking and dragging to highlight a specific section of the graph.

There are some events in the Venafi Platform category and the Venafi Framework category that are only available if you give the operational database account additional permissions in MSSQL Server, as described in the next section.

For information about using WebSDK for statistics reporting, see POST Stats/Query in the Developer's Guide.

Permissions for enhanced performance and scalability monitoring

In large deployments where you need to closely monitor performance and scalability, you can give the operational database account additional permissions in MSSQL Server. These permissions are optional, and are only recommended if you have a dedicated SQL server for Venafi Platform, because these permissions *could* give Venafi Platform the ability to query some limited details about other databases on the server.

IMPORTANT Venafi Platform **does not** collect **any** information about other databases on the server. However, because it is *possible*, we don't recommend you make these changes on shared database servers.

> Granting Database Owner (DBO) permissions in Venafi is safe because Venafi is a single-user environment. In multi-user environments, DBO permissions can be risky as they allow one user to modify others' data. However, in Venafi, only Venafi services access the database, so DBO permissions don't pose a risk to other users or databases on the same SQL server.

Giving the operational database account these permissions will allow Venafi Platform administrators to have readily available performance data on the Venafi Platform database, viewable in the Venafi Statistics MMC snap-in.

Giving enhanced reporting permissions in MSSQL

1. Log in to the database server with the database owner account.
2. In the **Object Explorer**, right-click on the database server container, then click **Properties**.
3. In the Page panel, click **Permissions**.
4. In the **Logins or roles** panel, click the name of the operational database account.
5. In the **Explicit** tab, click the **Grant** checkbox for the following permissions:
    - View any definition
    - View server state
6. Click **OK**.

Venafi Recycle Bin

For detailed information about the Venafi Recycle Bin MMC snap-in, see "Venafi Recycle Bin" on page 138.

Access Management

The access management node in Venafi Configuration Console (and the matching MMC snap-in) allows you to configure and manage access to Trust Protection Platform by way of Venafi's public APIs.

Equivalent functionality can be accessed using the OAUTH endpoints in the public API. For detailed information, see Grant management endpoints.

The access management overview page gives you a brief overview of the access that has already been granted, as well as a list of current global access management settings.

There are several possible actions on the overview page. Your ability to see or use them will depend on the role assigned to your identity. For information about roles in access management, see "Using roles for access management in Venafi Configuration Console" on page 396. Possible actions include:

- Change Global Settings
- Revoke User Grants
- Delete Identity Rules

Change Global Settings

Depending on your role, you may have the ability to view or edit global settings.

Tab	Field	Description
General	Username + Password	The client passes a username and password to the VEDAuth server. This is the same username and password that could be used to log in to the web console. Learn more about username and password authentication.
General	Integrated (Windows) Authentication	The client passes Windows credentials to Venafi for access. Learn more about Windows authentication.
General	Json Web Token (JWT)	A token in JSON format that is used to communicate between a trusted identity provider and Venafi Platform. Learn more about JWT authentication.
Certificate	Enabled	The caller passes a client certificate to Venafi for access. Learn more about certificate authentication.
Certificate	User identity field	The field from the X.509 certificate used to match the certificate with an identity in the system. ■ You can specify an SID as the certificate field and specify a backup field if the SID is not found.

Tab	Field	Description
		■ You can choose to always use a selected certificate field.
Certificate	Client certificate issuers	The CA(s) that are approved to issue client certificates for authentication. You can select one or more client certificate issuers to trust.
Device	Enabled	Device authorization allows for manual approval of devices in accordance with RFC 8628. Learn more about device authentication.
Device	Verification URI	The URI used for device authorization. This is the URI the device can use for verification, but doesn't include the user code. This response complies with section 3.2 of RFC 8628.
Device	Usercode verification URI	A verification URI that includes the user code, but is designed for non-textual transmission.
Grants	Access token validity	The duration of time between authentication prompts. Must be equal to or less than the grant validity. Access tokens automatically expire when the grant validity expires. This setting allows you to increase security by requiring periodic authentication to the system. When a token expires, if the access grant is still valid, a user can obtain a new token. Access tokens have a minimum validity period of one minute. They have an effective maximum validity period of the grant validity, since even if access tokens are still valid, once the grant validity expires, no access is granted. Learn more about the terms used on this tab.
Grants	Grant validity	The duration of time that the application will be able to access Venafi Platform. After the grant validity expires, an administrator will need to create a new application.

Tab	Field	Description
		A grant length can exceed the access token validity to require users to confirm their credentials more frequently.
Grants	Refresh enabled	When disabled, the system uses the *grant validity period* as both the *grant validity* and the *access token validity*. When enabled, the system allows the token validity to expire, requiring reauthentication for continued access.
Grants	Revoke if...	Allows you to conditionally revoke the grant if the access token is not used for a specified period of time.
WebSDK	API Statistics	Controls whether statistical information about your API usage is sent to Venafi. These statistics **only** include these three things: ■ The name of the endpoint. ■ The date and time the endpoint was accessed. ■ The duration of time it took for the endpoint to return data to you (if timing is enabled). No sensitive data is accessible to the statistics engine. See our statement on user analytics. Venafi uses this data to help us understand how Trust Protection Platform's APIs are being used so we can target our development efforts in the areas where our customers are using the product. Statistics are collected using a product called Pendo. Their data privacy policies apply in addition to the Venafi Trust Protection Platform privacy policy.
WebSDK	Session cache size	(Called **Session pool size** in the web console.) Specifies the number of concurrent sessions for API calls. If the number of simultaneous API calls exceeds the pool size, the oldest unused session is removed from the pool. Learn more about the terms used on this tab.

Tab	Field	Description
WebSDK	Validate/Expire every	The number of minutes each *access token* remains in memory. This functions essentially like a session cache, ensuring callers remain authorized to access the system. The default is five minutes. This field is used in conjunction with the **Validate Grant on Every API Access** setting. If the **Validate Grant on Every API Access** setting is *enabled*, this setting is ignored. If the **Validate Grant on Every API Access** setting is *disabled* (recommended), this setting applies.
WebSDK	Drop inactive sessions after	If a token is not used for this period of time, it is access permission is dropped. When the client reconnects, they will need to authenticate again.

Tab	Field	Description
WebSDK	Refresh user rights every	Determines how often user permissions are validated. While a token may remain valid, a caller's permissions within a scope may have changed. This setting determines how often the system validates these permissions. Longer times are more performant. Shorter times are more secure. The default is five minutes. Learn more about scopes and restrictions.
WebSDK	Validate grant on every API access	When unchecked (normal mode), credentials are cached for a specified amount of time (determined by the **Validate/Expire every** setting, above). When checked (strict mode), credentials are checked on every single API call, which has a measurable decrease in performance.[1] This setting is called **Expiration Mode** in the web console.
WebSDK	Enable API documentation	When you access the documentation on the Trust Protection Platform server in your environment, you can see detailed API documentation in Open API format when you visit the following URL: `https://your-server_url/vedsdk` You can disable is feature if you don't want users to be able to access the OpenAPI version of the documentation at the page listed above. When enabled, you can determine if you want the default viewer to use OpenAPI Epxlorer, Swagger, or ReDoc. Default: enabled, Open API 3.0.

[1]Because this feature queries the database for every API call, internal testing suggests that using strict mode (enabled) can increase call time by around 40%. While this may seem nominal for a single API call, in the aggregate it can dramatically affect performance for all components using the server.

Tab	Field	Description
		If this feature is enabled and users go to the `/vedsdk` URL, they will see the default viewer. However, they can use a different viewer by using an alternative URL. See Testing the Web SDK from the browser.

Revoke User Grants

Applies to the following roles: `Admin` and `Grant Admin`. Application owners need to click on their application in the Client Applications list to revoke user grants tied to their application.

If you want to immediately remove an identity's current grants (but not prevent them from obtaining new grants), use this action to specify which user should have their current grants revoked.

As in all identity fields, you can only see identities from the identity provider your current account is associated with. For example, the local `admin` user can't see active directory users, and a user logged in through active directory as an admin can't see local users.

Using the MMC snapin, you can configure your local machine to connect to your Venafi server using multiple identities at the same time, making it easy to see how different combinations of roles and scopes provide different access.

> **DID YOU KNOW?** You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.
>
> Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

Delete Identity Rules

Applies to the following roles: `Admin` and `Grant Admin`. Application owners need to click on their application in the Client Applications list to delete the rules tied to their application.

If you want to immediately remove an identity's ability to obtain new or refreshed grants, use this action to specify which user should prevented from obtaining any grants.

As in all identity fields, you can only see identities from the identity provider your current account is associated with. For example, the local `admin` user can't see active directory users, and a user logged in through active directory as an admin can't see local users.

> **DID YOU KNOW?** You can have snap-ins for multiple servers, allowing you to easily manage a complete cluster of Venafi servers, as well as servers in lower (development, test, etc.) environments.
>
> Additionally, since identities cannot see identities from other identity providers (local admins cannot see identities managed by Active Directory, for example), you can add multiple instances of the same snap-in for the same Venafi server, but with different user credentials. This allows you to manage users from multiple identity providers, or even see the rights and permissions granted to users within the same identity provider, but with different roles.

Using roles for access management in Venafi Configuration Console

When an identity accesses applications through the API, what they can do is determined by the role that is assigned to their identity.

List of oAuth roles

The following table lists the roles used for access management, and what rights they have.

Role	Access details
User	■ Any identity that has not specifically assigned a different role automatically has the User role. The User role cannot be assigned directly.
Auditor	■ Can see everything but change nothing ■ The Auditor role is automatically given to an identity that has Trust Protection Platform auditor rights. It can also be assigned directly to any identity.
Application Maintainer	■ Can modify the properties (such as name, scope, description) of specific applications ■ This role can be assigned by an Admin or by the Application Owner.
Application Owner	■ Can modify and delete applications they own ■ Can modify and delete rules related to applications they own ■ Can revoke grants issued for applications they own

Role	Access details
	■ Can assign and revoke the maintainer role for applications they own ■ Can assign and revoke the owner role for applications they own ■ This role can only be assigned by an Admin.
Mixed Owner/Maintainer	■ Indicates that the user is the Application Maintainer of at least one application and the Application Owner of at least one application. ■ This role cannot be directly assigned but is implied from a user being assigned the Application Owner and Application Maintainer roles.
Grant Admin	■ Can view all applications and rules ■ Can view and revoke all grants for a user ■ This role is intended for users or processes performing off-boarding tasks ■ This role can be assigned by an Admin.
Admin	■ Can create, modify and delete applications ■ Can create, modify and delete rules ■ Can issue and revoke grants ■ Can assign and revoke Application Maintainer and Application Owner roles for any application ■ Can assign and revoke the Admin role ■ Can configure global settings (session parameters, auth parameters, etc.) ■ Any master administrator automatically has this role, but it can also explicitly be assigned to regular identities by an existing OAuth Admin.

Assign a role to an identity

1. Connect to the Venafi Configuration Console on the Venafi server, or use the Venafi Access Management MMC snap-in to connect to the server you want to manage.
2. From the **Venafi Access Management** node, click **Roles**.

3. In the Actions panel, click **Assign...**.
4. Select the role you want to assign.
5. In the **To:** field, locate the user or group to be assigned the specified role.
6. [Conditional] If the new role is `Application Maintainer` or `Application Owner`, select which application this role applies to.
7. Click **OK**.

Revoke a role from an identity

1. Connect to the Venafi Configuration Console on the Venafi server, or use the Venafi Access Management MMC snap-in to connect to the server you want to manage.
2. From the Venafi Access Management node, click Roles.
3. Locate the role you want to revoke.
4. In the Actions panel, click **Revoke...**.
5. [Conditional] If a confirmation modal appears, click **Yes**.

Client Applications

Equivalent functionality

This topic covers the Client Applications node that is part of the Access Management feature in the Venafi Configuration Console and it's associated MMC snap-in.

Equivalent functionality is available in the web console. See "Integrating other systems with Venafi products" on page 752 for more information.

Equivalent functionality is also available in the Web SDK. See OAuth application endpoints for more information.

The Client Applications node allows you to manage your OAuth environment for API connections to Trust Protection Platform to create, update, manage, and delete applications.

Remember that what you can do with an application depends on the role assigned to the identity used to authenticate. See "Using roles for access management in Venafi Configuration Console" on page 396 for details.

The Applications panel lists all client applications in the system. Click on an application to see the Rule list for that application, which is a list of users with information about each user's scope and access.

Depending on your role, you may be able to perform the following actions.

Add a new application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. In the Actions panel, click **Add New Application...**.
3. Use the following table to help you set the required settings.

Order	Name	Description
1	ID	The ID of the application. This ID must be unique. It appears as the **Client ID** on the API Integrations list on the Trust Protection Platform web console, and as the *ID* in the API response.
2	Name	The name of the application.
3	Description	A description for the application.
4	Vendor	The name of the vendor that created the application.
5	Application URL	A URI to learn more about the application.
6	Required Scope	The minimum scope the application requires.
7	Maximum Scope	The maximum scope the application knows to use.
8	Override Global Defaults	Settings in this section are not required. You only need to modify if you want this application to behave differently than the global defaults.
9	Access tokens are valid for	The seconds a token for this application should be valid. Not passing a value uses the system default.
10	Grants are valid for	The seconds a grant for this application should be valid. Not passing a value uses the system default.
11	Grants can be renewed	`true` or `false` to set default behavior grant renewals. Not passing a value uses the system default.
12	Revoke if ... expired for	If an access token is expired and not renewed within the specified time frame, you can revoke the token.

Modify an existing application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Properties**.
4. Modify the application's settings, as desired.

   A table with descriptions for each filed is available in the previous section.
5. Click **OK**.

Add a new rule

Rules show the identities that have been given permission to request a grant for an application, along with what access the identities are allowed.

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Add New Rule...**.

4. Use the following table to help you set up the rule.

Order	Name	Description
1	Application	(Read Only) The application that can request access.
2	Trustee	The identity (user/group) that is allowed access.
3	Description	A description or explanation of the rule
4	Maximum Scope	The maximum scope the application is allowed to request.
5	Access tokens are valid for	The length of timean access token is valid. If this box is not checked, the system default at the time the grant is issued is applied.
6	Grants are valid for	The length of time, in seconds, until the grant expires and can no longer be renewed.If this box is not checked, the system default at the time the grant is issued is applied.
7	Grants can be renewed	If checked, a grant issued under the rule can be renewed. If not checked, it cannot not. If this box is not checked, the system default at the time the grant is issued is applied.

5. Click **Add**.

Delete an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Delete application...**.
4. [Conditional] If prompted, click **Yes** to confirm you want to delete the application.

Delete a single rule for an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.

   Wait for the application's rule list to load.

3. Click on the Rule you want to delete.
4. In the Actions panel, click **Delete rule...**.

Delete all rules for an application

1. In the Venafi Configuration Console or the Access Management snap-in, click the **Client Applications** node.
2. Click on an application in the applications list.
3. In the Actions panel, click **Delete all rules...**.
4. [Conditional] If prompted, click **Yes** to confirm you want to delete the application.

About JWT Mappings

A JSON Web Token (JWT; pronounced 'jot') is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. If Trust Protection Platform trusts the certificate used to sign the JWT, it trusts the identity information (claim) provided in the JWT.

JWT mappings are a way to tell Trust Protection Platform which issuers to trust, and how to map identity information in the claim to identities in Trust Protection Platform. This is a crucial part of the authentication process.

In addition to the general JWT mappings, you can also map Active Directory (AD) accounts to a JWT. This involves adding the AD user to the access management API integration and configuring the Access Management Snapin on either an admin's workstation or the TPP server. After these steps, you will be able to map to AD users when setting up a JWT mapping.

JWT Mappings operate in tandem with the central proxy configurations set at the root of the Platforms tree. See "About using an HTTP proxy" on page 784.

Want to know more? Learn about JSON web tokens in this Wikipedia article. Equivalent functionality is available in the WebSDK. See OAuth JWT mapping endpoints for details.

JWT mappings tell Trust Protection Platform which issuers to trust, and how to map identity information in the claim to identities in Trust Protection Platform.

Map AD Accounts to JWT

Mapping Active Directory (AD) accounts to a JWT mapping involves the following steps:

Method 1: Use an Admin's workstation

1. Add the AD user to the access management API integration.
2. Install VenafiMMC.msi on the Admin's workstation.
3. Launch mmc.exe and add the Venafi Access Management Snapin.

Method 2: Use the TPP Server

1. Add the AD user to the access management API integration.
2. Launch mmc.exe on the TPP server.
3. Add the Access Management Snapin.

After following either of these methods, you will be able to map to AD users when setting up a JWT mapping.

Add a new JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. In the Actions panel, click **Add New Mapping...**.

3. Use the following table to help you set the required settings.

Order	Name	Description
1		The name of the application
2		The Issuer URI to be trusted for this mapping
3	(Audience) Field	The name of the JWT field indicating the audience. You can click the Load JWT button if you want to paste in an existing JWT to automatically set these values.
4	(Audience) Must Match	The value that the audience field must match for the token to be accepted.
6	(Subscriber) Field	The name of the JWT field indicating the identity owning the token
7	(Subscriber) Map to	Select an identity for a token issued for this mapping. **NOTE** This field is evaluated as a RegEx (regular expression), not as a string.
8	(Subscriber) Extract identity	The regular expression to use to obtain the identity from the Subscriber Field. The first group matching the expression is used to determine the identity.

4. Click **Add**.

Edit an existing JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. Click on a JWT mapping in the list.
3. In the Actions panel, click **Properties**.
4. Modify the JWT's mapping settings, as desired.

   A table with descriptions for each filed is available in the previous section.
5. Click **OK**.

Delete a JWT mapping

1. In the Venafi Configuration Console or the Access Management snap-in, click the **JWT Mappings** node.
2. Click on a JWT mapping in the list.
3. In the Actions panel, click **Delete...**.
4. [Conditional] If a confirmation modal appears, click **Yes**.

Common terms in access management

Throughout the documentation we use the following terms when discussing the concept of access management for API applications.

Grant / Access Grant

A grant represents the right to access a resource URL (such as WebSDK, VedHSM). A grant can have limited lifetime, depending on configuration (default is one year), and a grant has attached to it what application is allowed to use it, and what scope for that application was granted. A grant is issued by the authentication server in exchange for valid credentials.

The Venafi Configuration Console and API use the term **grant**. The web console uses the term **access grant**. These terms are interchangeable.

Access Token / Token

OAuth uses bearer tokens for API authentication. The authentication server will return one or more tokens as part of an issued grant. Tokens infer access rights, and have a (configurable) limited lifetime. See the Auth REST for token management section for more information about getting tokens.

The Venafi Configuration Console and API use the term **access token**. The web console uses the term **token**. These terms are interchangeable.

Refresh Token

A refresh token might be supplied as part of the grant returned by the authorization server, if configured. Access Tokens have limited validity, and to ensure they don't get too much exposure, they often expire before the grant expires. In that case, a refresh token will have been provided when the grant was issued, and this refresh token can then be used to obtain a new access token (and a new refresh token).

Application (Integration)

Before an application can request a token, the application must be registered with the server. Unknown Client IDs/Applications cannot request grants.

In theTrust Protection Platform web console, Applications and Application IDs are referred to as *Integrations* and *Client IDs*.

Applications can be created in the web console from the API Integrations Inventory.

Scope

To allow fine-grained control over what operations an application is allowed to perform, each API endpoint requires a particular scope, and when requesting a grant, an application indicates what scope it requires. This allows you to restrict risk even if the user credentials used to obtain the grant provide wider permissions.

The scope controls what category of endpoints may be accessed. For example, `certificate` or `ssh`, or `statistics`.

Learn more about what scopes and restrictions are available.

Restrictions and Privileges

Within a scope, the caller is explicitly given the ability to do certain actions based on their privileges and restrictions.

If no privileges and restrictions are given for a particular scope, the caller will have *read* access to the related endpoints.

For example, a caller with the scope of certificate and no privileges and restrictions will be able to read certificate data, but will have no ability to take any actions. For the certificate scope, a caller can be given any combination of the following privileges and restrictions: **approve**, **delete**, **discovery**, **manage**, and **revoke**.

Other scopes have their own list of privileges and restrictions that can be granted for an identity.

Learn more about what scopes and restrictions are available.

Session cache size

You can limit the number of active sessions by setting the session cache size. In the web console, this is also called **session pool size**. When the cache size reaches it's limit, the oldest sessions are removed. A caller would need to refresh their token to access the application again.

Credentials

To obtain a grant, the authentication server requires credentials. The authentication server can be configured to accept any of the following as valid credentials:

- Username/Password
- User Certificate (The identity for the grant is obtained from the certificate)
- Windows Authentication (NTLM/Kerberos)
- Json Web Token (JWT) (The identity for the grant can be obtained from the JWT or be a fixed identity, based JWT contents)
- Device (unauthenticated request that requires manual approval)

Venafi Message Bus

The Venafi Message Bus provides near-instant notifications to other servers in the cluster about significant changes to the database. It is implemented using an MQTT message broker using a publish-subscribe messaging pattern. This allows all servers in the cluster near-instant visibility into the activities and configuration changes of other servers in the cluster.

Messages sent through Message Bus are informative, not authoritative and never contain any confidential data. The message is simply an instruction to other servers that *something* has changed, which allows the other servers to check the database to see *what* was changed, and then take action as needed. This also means that if there are connectivity issues in your network no important data is lost, because the important data isn't the MQTT message itself.

Message Bus is an integral part of the VPlatform service, and a core technology of Venafi Platform. It runs on Venafi servers when the VPlatform service is running. (This service is also known as Venafi Encryption Driver (VED) service.)

Message Bus provides several benefits. For example:

- Servers in the cluster always stay in sync. Configuration changes that used to require users to log out and log back in are now updated to all servers immediately without logging out and back in.

- Permissions are kept in sync. For example, if a user is given rights to a policy folder, those rights are updated across all servers almost instantly.
- Identities and access are constantly updated. When you remove a user from the system, they will lose access right away on all servers, without waiting for their session to refresh. Thus rights and permissions are always kept synchronized.

Configuration Types

Message Bus operates in one of two ways to accommodate all deployment scenarios:

- **Self-Hosted (mesh style).** In this default configuration, each server in the cluster communicates with all other servers in the cluster directly by subscribing to every other server's broker. Every message published from the remote brokers will be passed to the local brokers. This configuration is supported natively by Venafi Platform, and requires no additional configuration as long as the bus port is open to allow communication with all other servers in the cluster. Most customers use this configuration method.
- **Central MQTT Broker (hub-and-spoke style).** In this configuration, all servers in the cluster publish and subscribe to an external MQTTv5 broker, and the broker distributes the messages to all servers in the cluster. This deployment option is provided for customers already using an external MQTTv5 broker and who are required to use that service, or who don't want another broker working on their network. Another reason you might use hub-and-spoke configuration is if your cluster cannot communicate between all servers using the configured port, but the servers can all reach the same external broker. You will need connection information to your central MQTT broker to use this configuration type.

Message Bus is not optional. It is an integral part of Venafi Platform. For new installations of Venafi Platform, Message Bus is configured during the installation steps. For upgrades, the *first* server in the cluster that is upgraded to version 23.3 (or higher) will require you to configure it. Subsequent servers will not require Message Bus configuration on upgrade or installation.

Network Requirements for Message Bus

Message Bus requires correct network configuration. Depending on whether you are using mesh mode or hub-and-spoke mode:

- **Self-Hosted (mesh style).** All servers must be able to communicate with each other over the configured port (default is 8883 for TLS, or port 1883 if you are using an unencrypted bus). Almost all configuration issues are due to incorrect port configuration.

- **Central MQTT Broker (hub-and-spoke style).** Each server must be able to communicate with the central MQTTv5 server over the configured port (default is 8883 for TLS, 1883 if you are using an unencrypted bus.

We suggest you get the network configured correctly before upgrading. Once a server has been upgraded to 23.3 (or higher), you can see if there are any communication issues by looking at the Message Bus node in Venafi Configuration Console where there is a graphical representation of your network which makes it easy to see where any communication issues are detected.

What's Next?

If you are just getting started with Message Bus, see "Modifying Message Bus configuration settings" below.

For details about your Message Bus health and status, see "Working with Message Bus" on page 412.

Modifying Message Bus configuration settings

The information on this page will help you configure Message Bus for your server environment. In its simplest default configuration, Message Bus just works as long as the IANA-assigned port for MQTT (port 1883 for unencrypted, or port 8883 for TLS-encrypted) is open on all Venafi servers. That means you don't necessarily need to configure Message Bus after installation or upgrade.

This topic discusses additional configuration options related to Message Bus you can make in Venafi Configuration Console post installation (or upgrade).

Before you Make modifications to Message Bus configuration

Before modifying the default Message Bus configuration, you need to know the answers to the following questions:

- Do you want to use encrypted MQTT traffic or unencrypted MQTT traffic? (The default is TLS encrypted.)

  While the bus itself doesn't exchange security-sensitive information, the credentials used to authenticate to MQTT might get passed over the wire, which is why we recommend using encrypted communication.

- Do you want to use the default ports? The default port for encrypted MQTT traffic is 8883. The suggested port for unencrypted MQTT traffic is 1883. These are the IANA-assigned ports for MQTT, set by the ISO standard ISO/IEC 20922:2016.[1]

  You'd only want to modify this setting if you have previously assigned the default port for another purpose, or if your network security team asks you to use a different port.

- Do you want to use a self-hosted (mesh) configuration, or do you want to use a central MQTT broker service (hub and spoke) configuration? (The default is self-hosted.)

  Self-hosted (mesh mode) is entirely provided by Venafi Platform. The only reason to use a central MQTT broker is if you are already using one in your organization, and you want to integrate that MQTT broker with Venafi Platform.

- If you are using a central MQTT broker, are you authenticating with a user name and password, or are you using a certificate? If a certificate, do you have the PFX certificate file?

To modify Message Bus configuration settings

1. On one of the Venafi servers in your cluster, open Venafi Configuration Console.
2. While on the root node, click the **Configure Message Bus** action in the **Actions panel**.
3. Verify the port number.

   Venafi Platform automatically assigns the default MQTT port for encrypted or unencrypted traffic, depending on your TLS setting. You likely won't need to modify this setting.
4. [Optional] If you require *unencrypted* communication between servers, **Disable TLS**.
5. For Self-Hosted (Mesh) connections between servers:
   a. Click the **Self-Hosted (Mesh)** option, if not already selected.
   b. If you need to change the hostname, click **Override Hostname**.

What is Override Hostname?

A hostname is one way a computer is uniquely identified on a network. In mesh mode, servers need to be able to communicate with each other, and they identify each server by its hostname.

[1]The ISO/IEC 20922:2016 standard is available on ISO.org at https://www.iso.org/standard/69466.html.

The default hostname that Venafi Configuration Console detects for a server might not resolve to the correct address for all servers. An example of this is when using a load balancer, where multiple servers self-identify with the hostname of the load balancer, not the server itself.

To address this, you can use the **Override Hostname** option, which allows you to enter a fully-qualified domain name (FQDN) that resolves to this server. If you are using TLS, you cannot use an IP address in this field.

i. Review the Detected name. This is the name that Venafi Configuration Console detected for this host. You can't edit this field.

ii. Enter a fully-qualified domain name to use to connect to this server in the **Override with** field.

iii. Click **Save**.

c. Click **Save**.

d. Ensure all servers in the cluster can communicate to each other using the selected port. In mesh mode all servers need to be able to reach all other servers in the cluster over the specified port. The Message Bus node in VCC will help you identify any communication issues between servers in the cluster.

That is all that is needed to configure Message Bus in mesh mode. You can skip the next step.

6. For Central MQTT Broker (Hub & Spoke) connections between servers:

a. In the **Central MQTT Broker** field, enter the URL of the central MQTT broker.

b. If multiple clusters of Venafi servers are sharing the same central MQTT broker, select a unique **ID** for this cluster. This will ensure the bus correctly interprets which bus messages are intended for this particular server cluster. Other clusters must use a different ID.

For example, if you have a cluster in your development environment and a different cluster in your production environment sharing the same broker, you would assign different ID values to these clusters so the subscribers can differentiate between clusters.

c. Make sure the servers can reach the central MQTT broker over the specified port by ensuring the firewall is configured to allow traffic over that port.

It's easy to see if there are communication issues if you look at the bus overview. If you see all green check marks your ports are configured correctly. If you see red X marks, there is additional information to help you diagnose the issue. See "Working with Message Bus" below for details on viewing communication status and diagnosing potential issues.

d. If your broker requires authentication, select an **MQTT Authentication** type.
   i. To use a user name an password:
      i. Click the **Username** option.
      ii. Add your **Username** and **Password**.
   ii. To use a certificate:
      i. Click the **Certificate** option.
      ii. Click the **Load PFX** button.
      iii. Browse to the location of your PFX file and select it.
      iv. Enter the Password for your PFX file.

      The certificate loads, and you can see its data.
      v. If this is the correct certificate, click **Ok**.
e. Click **Validate**to verify communication with the central broker.

Working with Message Bus

The Message Bus node in Venafi Configuration Console shows the status of communications between servers in the cluster. As you hover over the nodes in your cluster, you can see detailed information about the servers and their connectivity to the bus.

Mesh mode

Icon	Status	Description
	Blocked	The server is in the cluster, but cannot communicate with any other servers. For example, the designated port is not open, or the Venafi Platform service might not be running on the server, or the server might be offline.
	Cant Reach All	The server is participating in the bus, but it is not able to reach one or more other servers in the cluster.
✓	Connected	The server is participating in the bus and can communicate with all servers in the cluster.

If you are experiencing connectivity issues, make sure that the firewall settings allow communication over the specified port. In mesh mode, all servers need to be able to reach all other servers in the cluster over the assigned port.

As you hover over servers in the cluster, you will be able to see details about any connectivity issues the servers are encountering. For example, if you hover over a server with a yellow warning symbol, you can see details about which servers it can connect to and which ones it cannot connect to.

Hub-and-Spoke mode

Icon	Status	Description
	Not Connected	The server is not participating on the bus. This may be because the server is offline, or because it is on an older version of Venafi Platform that doesn't support Message Bus, or because the firewall doesn't allow connection to the central broker over the specified port.
✓	Connected	The server is participating in the bus and can communicate with the central MQTT broker.

If you are connected to the server that is not able to communicate with the central MQTT broker, all other servers in the cluster will appear to be disconnected, since this server cannot get information from the broker about the other servers in the bus. If this applies to you, try logging in to another server in the cluster to check its connectivity to help you determine whether the problem is with this server's configuration, or with the central broker.

If you are experiencing connectivity issues, make sure the firewall settings allow communication over the specified port. In central broker mode, each server needs to be able to reach the central MQTT broker over the specified port.

Troubleshooting communication issues

Message Bus is designed to require very little maintenance, so most issues boil down to the following connectivity issues:

- Firewall / Port issues. If the specified ports are not open, the bus nodes won't be able to connect.
- Server status. If the server is powered off, or if the Venafi Platform service isn't running, then the bus clearly can't get updates from the server.

If you need to send a network administrator information to help troubleshoot network connectivity issues, you can click the **Copy health information** link in the **Actions** panel. Connectivity information will be copied to the clipboard so you can send it to the network administrator.

You can quickly see what applications and services are running on each node by clicking the node or click on the server in the graph. **Copy status information** link in the **Actions** panel.

All status information can be copied to the clip board by clicking **Copy Status Information**.

The information from these two links can help you and your network administrators troubleshoot any connectivity issues in the cluster.

Individual engine nodes

If you expand the Message Bus node, the list expands to show all nodes in the cluster. Click on any node to see detailed information about that server.

You see a detailed Engine Status table. It shows services, applications, and service modules running on that server, as well as how long they are have been running and their process identity.

In the Actions panel you can see a description of the selected engine, as well as the measured database latency for that server.

You can specify the hostname used in the mesh by clicking **Set mesh hostname** in the **Actions** panel.

What is Override Hostname?

A hostname is one way a computer is uniquely identified on a network. In mesh mode, servers need to be able to communicate with each other, and they identify each server by its hostname.

The default hostname that Venafi Configuration Console detects for a server might not resolve to the correct address for all servers. An example of this is when using a load balancer, where multiple servers self-identify with the hostname of the load balancer, not the server itself.

To address this, you can use the **Override Hostname** option, which allows you to enter a fully-qualified domain name (FQDN) that resolves to this server. If you are using TLS, you cannot use an IP address in this field.

1. Review the Detected name. This is the name that Venafi Configuration Console detected for this host. You can't edit this field.
2. Enter a fully-qualified domain name to use to connect to this server in the **Override with** field.
3. Click **Save**.

Root Node

On the root node of the Venafi Configuration Console there is a panel that shows the configuration status of the Message Bus. There you can see:

- The operating mode (self-hosted mesh or central MQTT broker)
- The port
- Encryption status (TLS yes/no)
- The hostname of the current server

> **TIP** If you are on the root node and you change the port, you are changing the port for *all servers in the cluster*. If you are in child node and you change the port, you are only changing it for *that specific server*.

Health Check

Message Bus periodically checks to verify that the bus is working as expected. These checks occur five minutes after the VPlatform service starts, and then again every hour. If there is an issue, Venafi Platform will wait fifteen minutes and check again. If there is still an issue, Venafi Platform sends an e-mail notification indicating that there is a health issue with the bus[1].

---

[1]This assumes you have configured SMTP, as no e-mail notifications can be sent by Venafi Platform until SMTP settings have been properly configured.

IMPORTANT If your first installation of Venafi Platform was version 23.1 or older, these e-mail notifications are **not** enabled by default. For information on enabling specific notification rules, see Customizing email notifications. Note that there is one default email notification rule for central configuration, and a different default email notification rule for mesh configuration. Make sure you enable the correct one for your setup.

Tools

The Tools node of Venafi Configuration Console (VCC) contains system tools that help you manage your environment. This node is also available as an MMC snap-in.

As of 25.1, there is only one tool in this node, Logging.

Logging controls all notifications and logging features of Venafi Platform including e-mail templates and e-mail notifications. While most logging and notification features are covered in the topics that follow, you can always refer to the Venafi Log Server Administration Guide (version 25.1) for comprehensive information about the entire logging system.

TIP One frequently used feature of the Tools node is to customize existing log events. To learn more about that, see "Customizing event definitions" on page 425.

Understanding system logging and notifications

With Venafi Trust Protection Platform™, you're not just monitoring and managing your encryption resources—you're also keeping track of those activities and passing along important information about system events as they occur. The platform's log server monitors events and centralizes the logged information. This makes it easier for you to review and assess how your encryption system is performing. Whether you're auditing, troubleshooting, or conducting operational reviews, these logs are your go-to resource.

You can also configure notifications for specific events. By defining notification rules, you can route information about events to a variety of channels like SMTP, SNMP, File, MS SQL, or Sysog, keeping you updated about the events you care about in whatever formats you choose.

Logging overview

The Trust Protection Platform logging system consists of the following components:

- **Events**: Describe an error or status. For example, an event fires when a certificate is about to expire.
- **Venafi log server**: Monitors events, processes logs, and manages sending alert information to specified destinations.
- **Default SQL Channel** : Stores a history of events as a log to a database. These logs can be filtered using a Filter Channel to reduce unwanted or unhelpful event logs.
- **Notification Rules**: Determine which events are forwarded to channels for processing and which events are ignored.
- **Channels**: Manage the delivery of processed log messages in a variety of formats.

The component in Venafi Platform process events, and those events are reviewed by the logging servers. The basic logging of events happens in the default channel. Additionally, based on notification rules, information about events can be passed to channels for delivery to an external system, such as a mail server.

Let's walk through an example:

Imagine Venafi Platform detects a certificate nearing its renewal date. This is an *event*. This information is stored to the *default channel*. Additionally, the log server finds a *notification rule* that matches this event. The notification rule is linked to a specific SMTP *channel*, so the log server passes the information along to the linked SMTP channel.

The SMTP channel is an email notification channel. It uses templates, macros, and message settings to send an email notification to a specified recipient.

If the log server found multiple notification rules for the event, all matching rules would be triggered, and their linked channels would receive the information about the event to process based on their channel settings. So, if there is a matching notification rule tied to a File channel, the event log will be saved to a text file on the corresponding file system.

These are just a couple of examples. Venafi Platform supports several other types of channels for delivering event information based on your organizational needs.

Log server

The Venafi log server serves as the heart of the event logging and processing system, ensuring the events you care about don't go unrecorded.

For a deep dive into managing the Log server, check out "Managing the log server" on page 429.

As a brief overview, the log server:

- **Monitors events**. As Venafi components manage your encryption assets the log server tracks all the events to see if there is a notification rule for each event, and if there is, sends the information to the proper channel for processing.
- **Maintains an audit trail**. Every event gets logged to the default channel, giving you a comprehensive record of all system activities and events. By default, this is an SQL Server channel, and events are stored in either the Venafi Platform database, or another database you configure, however you can use a different channel, like a File channel, as your default if you prefer.
- **Takes actions specified by channels**. When notification rules are triggered by events, the event data is processed by the channel specified in the rule. The log server follows the channel configuration settings to transmit the event log information to the specified destination.

Default channel

Venafi Platform comes configured to store logged event data in its own MS SQL database though a channel called Default MS SQL Channel.

SQL channels store a set of tables and views that automatically capture log information about all system events.

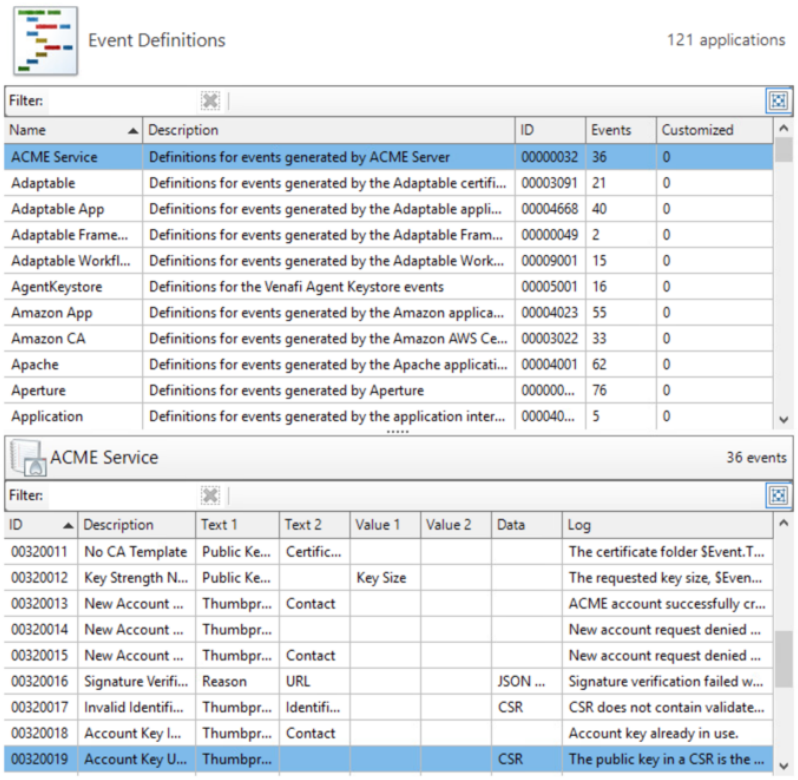
If you need to manage a high volume of events, you can create custom SQL channels to direct logs to other databases. If you need, you can use a Filter channel to ensure you filter out events that aren't interesting to you because of their low severity, or because of some other criteria.

These settings are designed to help you get the right information about the events you care about to the people or systems that need to know about them, and are a critical part of your machine identity management strategy.

For step-by-step instructions on setting up a SQL Server channel, refer to "Creating a SQL Server log channel" on page 448.

Event definitions for server components

All server components have events. The events that the log server tracks are listed in Venafi Configuration Console in the Event Definitions node (**Tools** > **Logging** > **Event Definitions**).



Venafi components are listed in the top table. Click a component to see all the events that the log server tracks for that component. Double-click an event to see how you can customize the description and "translation" of the event. The translation is just a friendly version of the technical log .

As with other tables in VCC (and the MMC snap-in), you can use standard table tools to help you find events in the table. This includes the Filter box, column sorting, and grouping by columns.

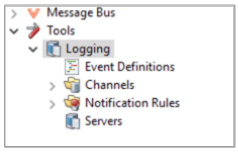
As you make changes, rest assured that your changes will be preserved when you upgrade, and that if you ever want to go back to the default description or translation, it's easy to reset. (The blue arrows on the right will reset the field to its default state.)

Most organizations find the default event definitions meet their operational requirements, so they don't need to customize them, however know that if your needs are different, you can make the needed changes.

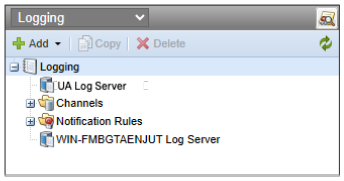
> **NOTE** You must have `Read` permissions to view the objects in the Logging tree, and you must have `Read, Write` if you want to edit them.

Logging tree

If you've used Venafi Platform versions 23.1 or older, you may be familiar with the Logging tree, accessible from the Policy Tree menu. Starting with version 23.3, we recommend you use Venafi Configuration Console (VCC) for modifying logging settings. VCC provides advanced features, and is where you can control all aspects of your log environment, including creating and managing channels, message templates, notification rules and more.



VCC's Tools node



Web Console's Policy Tree

Venafi Configuration Console or the Tools MMC Snap-in?

For consistency, the instructions in this guide always refer to the **Tools** node as being a component in Venafi Configuration Console (VCC). Using VCC requires you to open a session on the Venafi server itself.

The Tools node of VCC is also available as an MMC snap-in from any Windows computer that can make API calls to the Venafi server's SDK endpoint (`[yourserver]/vedsdk`). If you are using the Tools MMC snap-in, when you see instructions to open the Tools node in VCC, you can open the corresponding snap-in collection on your local Windows machine instead, then follow the rest of the instructions as printed.

There is *no difference* in functionality between using VCC or the snap-in collections. Many customers have found that using the various MMC snap-ins make administering their server clusters much more convenient.

To learn how to install and use all the snap-ins, including Tools, see "Install the Venafi MMC Snap-In Collection" on page 363.

Event definitions VCC Node

As discussed in "Event definitions for server components" on page 419, event definitions tell the log server what to pay attention to, and what information to pass along to a notification rule, if the logging server finds a notification rule based on that event.

Channels VCC Node

Channels define the way logs are sent to the correct destinations. The Channels node shows a list of all configured channels. You can edit existing channels and you can create new ones as needed.

The following channels are the possible destinations for a log or notification:

- **SQL Server**. The SQL Server channel allows you to specify a table in a database to store matching log and event notifications. You can write to a table in Venafi's database, or you can use custom connection information to connect to an external database.
- **SMTP**. The SMTP channel lets you send email messages (both plain text and HTML) to specified users. SMTP channels are based on templates, making it very easy to use the same images and style settings for groups of related messages.
- **Adaptable**. Using an Adaptable Channel PowerShell script, you can programmatically send logging events to any destination of your choice, even when it isn't one of the pre-defined channel options in Venafi Platform. For example, if you want to trigger an incident in your ITSM system, you can create a PowerShell script that connects with your ITSM incident management software.
- **File**. Stores notification text in a flat file in the log server's file system or on a network share the log server can access.
- **Filter**. Usually used in combination with the default channel, a filter channel is unique because its target is another channel. The filter channel checks event logs to enure logs you are not interested in aren't allowed to pass along to the destination channel. Other channels typically don't need a filter channel, because the notification rule contains the criteria used to determine if the log should be sent to the target channel
- **SNMP**. The SNMP channel lets you direct traps to an SNMP server. SNMP is a protocol that allows an agent to send an unrequested message to the manager to notify about an important event. Venafi server supports all versions of SNMP.
- **Syslog**. The Syslog channel sends log information to a target host. All variants are supported.

Notification Rules VCC Node

When events happen, the log server reviews the notification rules to determine if the event information should be sent to a channel for distribution. A notification rule is always linked to one or more channels, as notification rules route log messages about events to channels. A notification rule without any channels will not trigger any logging.

Because notification rules can trigger one or more channels, a single notification rule may be sent to multiple channels, which could result in one or more email notifications as well as other logs stored on a file system or database.

Notification rules can also be disabled, in which case they are ignored when the log server processes events.

If you modify the default settings for a notification rule, its changes will be preserved during system upgrades.

Servers VCC Node

The servers node shows you all the servers in your cluster. In large environments, you may have one or more servers dedicated to logging, and this node lets you enable or disable logging on individual servers.

Information about multiple log servers

Venafi Platform supports more than one log server, however you should be aware of the following if you are using multiple log servers:

- All log servers need to use the same default channel. When there are multiple log servers, you can't know which log server will process a notification rule. If you have different default channels on your servers, the logs will be erratic, and finding event logs will be quite difficult.

  If you have multiple log servers with different default channels, you'll see a warning in the **Attention Required** node in VCC.

- If you are using a File channel, you should strongly consider only using a *single* log server. If your file output is saved locally on the Venafi server, you would have incomplete logs that you would need to combine for an accurate, complete log. If your file output is saved on a shared network drive, your

log servers will constantly be competing to write to the file, which will result in errors and incomplete logs.

Log events

Log events are generated by Trust Protection Platform components as well as custom add-ons provided by Venafi, our partners, or customer organizations.

All log events have a standardized set of fields. This allows the log server to store events in a database and query events across all sources.

When an event occurs, the following sequence of events beings.

1. A Trust Protection Platform component serves an event to the Log API.
2. If the event's severity level is `Debug`, and the Debug setting is disabled, it is discarded.
3. The Log API sends the event information to the MSSQL Service Broker Queue for processing.
4. The log server periodically checks the queue.
5. The log server sends the event to the default log channel.
6. The log server applies matching notification rules. This may trigger sending the event information to the corresponding channels.

Event IDs and severity levels

Events have unique event IDs which are 32-bit numbers expressed in hexadecimal. The first four digits define the component. Using these first four characters, you can see how events are grouped by the component that triggers the event, and you can see other events from the same source.

You can see the event ID when you review the event in Logging's Event Definitions node .

All events also have a defined severity level, which helps you assess how critical Venafi considers the event. You can use severity levels in notification rules to help you discover the most important logs.

Severity Name	Critical Rating
Emergency	*Most critical*
Alert	
Critical	
Error	
Warning	
Notice	
Info	
Debug	*Least critical*

Customizing event definitions

You can use the Venafi Configuration Console (or the Logging MMC snapin) to customize existing event definitions.

To customize an existing event definition

1. Open the Venafi Configuration Console (or the Tools MMC snapin), and open the **Tools** node.
2. Click the **Event Definitions** node.
3. In the bottom panel, double click on an **Event**.
4. You can customize both the **Description** and the **Translation**.

Macros are allowed. You can see what content will be provided in the macros when you look at the event definition.

For example, if the content for **Text 2** is "Contact", you could incorporate the corresponding macro, `$Event.Text2$`, like this:

> For additional information, please reach out to $Event.Text2$.

If you incorporated this into an email notification, the resulting paragraph would replace `$Event.Text2$` with the contact's name, and might look like this:

> For additional information, please reach out to Jon Smith.

5. When you're done, click **Apply**.

Resetting to original event definitions

When you change an event definition, it gets marked as "customized" and is protected from changing during upgrade. You can revert an event definition to the default by clicking the Undo arrow next to the event description or the event translation.

> **TIP** If you are having trouble with events after upgrade, it's possible that the default behavior for an event changed, and that is conflicting with a customization you have made. Check to see if you have any customized events by looking on the Events Definitions panel, and reviewing the Customized column. If there are customized events, try resetting them to the default to see if that resolves your issue.

Creating custom logging event definitions

Out of the box, Venafi Platform provides an extensive list of event definitions, however if you find that you need an event definition that is not available you can create your own definitions. For example, if you are a third-party developer, you may want to create logging events tied to the features you are developing.

Event definitions describe the ongoing progress about Venafi or your own add-applications. When an event fires, the Logging application formats the event and it appears on a Policy folder **General** tab and in a MSSQL Logging channel, such as the Default SQL Channel. **When you upgrade to a future version of Trust Protection Platform, any add-on events automatically migrate.**

IMPORTANT We strongly recommend that you avoid making changes directly to the Log schema for events. Instead, you can customize log events that appear in the **Tools > Event Definitions** node of the Venafi Configuration Console (or the Logging MMC snapin). For more information, see "Customizing event definitions" on page 425.

When adding your own logging events:

- Make sure each add-on has its own unique Group ID. Use the reserved decimal range of `0200`-`0299`.
- *EventID*s must be unique. For example, you can use Group ID `0200` and assign EventIDs from `0200000` through `0200FFFF`.
- Comma separate each field and leave unnecessary fields blank.
- Use macros to allow the Logging application to add dynamic information. For more information, see Using the $Event.Formatter$ macro. For example:

  ```
  02001FAF,Custom App - Certificate Expiration Processing,,,,,,,,,,"Service module for the engine $CN [$EHvent.Component$]$ is examining certificates for expiration."
  ```

  When this event triggers, the Log server records the following event:

  ```
  127.0.0.1, 17/08/2009 22:17:42: Service module for the engine Jupiter is examining certificates for expiration.
  ```

5

Managing the log server

The Venafi Platform log server manages the flow of information to the default channel, interprets notification rules, and utilizes channels to deliver targeted log messages based on those rules. It reviews defined events, then logs all events to the default log channel to ensure there is a complete audit trail of all system operations and events. Once an event is logged to the default channel, the log server checks notification rules to see if any rules match. If there is a matching notification rule, the log server forwards the log data to the appropriate channels, which deliver the log to the defined service, location, or person.

The Servers node shows the log servers in the cluster, and is where you can specify the default log channel.

As a safeguard, whenever you make configuration changes to the default log channel, you need to restart the log server service. All other channel changes will refresh after configuration changes, and do not require a service restart.

This chapter contains the following topics:

Reviewing log events in VCC

You can use the Venafi Configuration Console to review events in the following ways:

- View all events or create a custom view that filters just the events you want.
- Create custom views of events you want
- Save events to a .CSV file for reference
- Import earlier-saved .CSV event files
- View statistics about events
- See an overview of events logged over recent time periods (one hour, one day, one week). This is a useful feature that gives you a quick overview of your system's event history without needing to read individual logs.

To review log events in VCC

1. In Venafi Configuration Console (VCC), open the **Events** node.

   > **TIP** If you are using the MMC snap-ins, be aware that Events is a separate snap-in from Tools, and has to be loaded separately.

2. The following table shows some of the things you can do to review recent events.

Action	Description
Report events by time period, and occurrences	Review the Log Summary table. ◦ **Event Type** describes an event severity. If there are any logged events during the last week for that event type, you see a plus icon. Click that to see the events in that categorty. ◦ **Event ID** provides the event message. ◦ **Source** identifies the component that fired the event. ◦ **Last hour**, **24 hours**, **7 days** show the cumulative number of occurrences for a time period.
Sort, group, and Drill Down	Click on a column header to sort by that column.

Action	Description
	Right-click on a column header to see grouping options. You can group by this column, or you can Show GroupBox, which allows you to create advanced grouping rules that can help you locate events quickly. Right-click on cell data to use the Drill Down feature. The Drill Down options depend on the type of information in the cell. For example, clicking on a source value in the All Events list lets you see all events from that source, or from the same component, or during a specified time frame. Clicking on a certificate renewal event lets you see all the other events that were tied to that certificate's renewal action (like workflow approvals, and so on). As you use Drill Down you'll see temporary views based on your drill-down criteria appear in the Events node. (These are session-specific and are removed when you close VCC or the snap-in.)
Show all events	Click **All Events**. The same sorting, grouping, and Drill Down features are available for All Events.
Create a custom View	a. Right click **Custom Views** and select **Create Custom View**. Filter, and then click **OK**. Filters: • **Event level** describes the event severity. • **Event sources** match an Event Definition in the Policy Tree Logging tree. • **Limit to** shows the number of the newest events. b. On the **Save Filter to Custom View** screen, type a **Name** and **Description**, and then select or create a VCC folder for the log. c. Click **OK**.

Action	Description
Create custom view filters	a. Click **Custom Views** and the view name. b. (Optional) In the **Actions** pane, click **Filter Custom View**, select options as appropriate, and then click **OK**.
Export a custom CSV log	a. Open the custom view and in the **Actions** pane, click **Save Event Log as**. b. Specify a path, and then click **Save**.
Import a custom CSV log	a. Click a custom view and in the **Actions** pane, click **Open Saved Log.** b. Specify a path, and then click **Open**.

For more information about using the Venafi Event Viewer, see "Venafi Event Viewer" on page 374.

Manually stopping and starting the log server service

The Venafi log server service manages event logging and notifications. If you need to stop, start, or restart the log server service, use the following instructions.

If the log service is running, and you want to restart it

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel.
3. Click the **Restart** action.

   The service will stop, then restart. The process is complete when you see the service change back to **Running**.

To manually stop the log server service

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel.
3. Click the **Stop** action.

   This sets the status to **Stopped**.

To manually start the log server service

1. In Venafi Configuration Console, open the **Product** node.
2. Click the **Logging** component in the middle panel
3. Click the **Start** action in the right panel.

   This sets the status to **Running**.

Configuring the log server

The log server represents the service that manages all logging and notification functions for a particular server. The log server is automatically created when you install Trust Protection Platform on a server and can be seen in Venafi Configuration Console (VCC) under **Tools** > **Logging** > **Servers**. Each server in the cluster has a separate server entry.

> **IMPORTANT** Whenever you make configuration changes to the default log channel, the Logging service requires a restart. All other channel changes will refresh after configuration changes without requiring a restart of the Logging service.

To configure the Log Server using VCC

1. In Venafi Configuration Console (VCC), open the **Tools** > **Logging** > **Servers** node.
2. From the list of log servers, click the specific server you want to configure.
3. Click **Properties** in the **Actions** panel.
4. Make the configuration changes.

   Refer to the table below for the options.
5. Click **OK** or **Apply**.

Property	Description
Description	A friendly description for the server.[1]
Default Channel	The Venafi log server records all events to a log table in the Trust Protection Platform database. If you want to see log events onscreen, you must use a database channel as your default log channel.[2] **IMPORTANT** You must ensure the database server that stores the channel data does not run out of disk space. If the server runs out of disk space, the log server cannot operate. The space you need for your log store depends on a number of factors that include, but are not limited to, how many events per second you are storing and how long you want to keep the data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring. **WARNING!** If you are using your Venafi server as your logging server, if your server runs out of disk space, the *entire set* of Venafi services on that server will stop working.
Server Disabled	Controls whether this server will process log events or not.

You can see the server's details in the bottom panel including the channels and notification rules that this log server processes.

Controlling the size of the log

Trust Protection Platform logs event data into a centralized database so you can review and evaluate your system activity. The logged information is helpful for auditing, troubleshooting, and operational reviews.

Typically, the channel that is used is the Default SQL Channel. Its job is to log all events.[3] Over time, the number of log entries can accumulate, taking up disk space and making the data more difficult to search and use. Minimizing the total number of logged events in the database improves the usability of the data and minimizes disk space usage.

---

[1] On the Actions panel of the main Log Servers page you have an option to rename the log server to change the server's name in the list.
[2] Technically you can also use a filter channel as your default log channel as long as it points to an SQL database channel.
[3] In its default configuration, an SQL Server channel logs all system events. However, you can use a Filter channel to discard some events so your logs are more relevant and take up less space.

IMPORTANT If you do not want to delete logged events at all, you can disable log expiration altogether. However, if your log file is not managed correctly, it can grow large enough to use up all remaining disk space and significantly impact server performance.

You can specify how many days each log entry is kept before it is deleted automatically. When a logged event exceeds the number of days you specify, the log entry is deleted permanently.

NOTE The default setting for log event deletion is 90 days. You can set any value between 0 and 3650. A setting of 0—or if you leave the value blank—disables log expiration.

To configure log event expiration in VCC

1. In Venafi Configuration Console, navigate to **Tools** > **Logging** > **Channels**.
2. Click **Default SQL Channel** in the center panel.
3. Click **Properties** in the Actions panel.
4. In the **Automatically delete records older than** field, set the number of days to maintain logs for this channel.

   The default number of days is 90.
5. To disable automatic deletion of logs, uncheck the **Automatically delete records ...** option.
6. Click **OK**.

TIP Log expiration can also be set during the initial installation of Venafi Platform, and is one of the settings in the XML answer file you can use to provide initial configuration information for new servers.

Setting up SMTP settings for outbound email connections

Venafi Platform has powerful logging capabilities, with a variety of methods of delivery. After database logging, the most popular form of notifications is via email.

Venafi Platform will *not* be able to send email notifications for log channels or for the reporting service until you configure the outbound SMTP server settings, as described below.

The SMTP server settings you want to use may be the same for both log channels and the reporting service, however you need to set up both if you are using both features. Keeping the configurations separate allows you to use different email settings for the different purposes.

Configuring the SMTP Default Connectors for Log Channels and Reporting in VCC

1. In Venafi Configuration Console, open the **Connectors** node.
2. In the SMTP Default Connectors section, click the connector you want to configure.
    - **Log Channels**. This connector controls the SMTP email configuration for all SMTP Log channels. For more information, see "Setting up notification channels" on page 439
    - **Reporting**. This connector controls the SMTP email configuration for all Reporting service modules.
3. Click **Properties**.
4. If prompted, log in to Venafi Platform using an account with system administrator permissions.

5. Enter the SMTP Server information as outlined in the table below.

Field	Description
Host	Enter the SMTP host name or IP address. For example: `smtp.example.com` or `127.0.0.1`.
Port	Enter the port to use for the SMTP connection. The default port for SMTP connection is 25, which does *not* encrypt the connection. To use Secure TLS communication, you cannot use port 25. Here are the three standard SMTP ports: ◦ Port 25. (Default) This is a non-secure default SMTP port. ◦ Port 465. This port securely sends email via SMTP by SSL/TLS. ◦ Port 587. This is the successor port of port 465 and is often seen as the default transmission channel for secure SMTP connections. **About secure SMTP connections** Venafi uses SMTP Authentication for outbound email. We are investigating support for OAuth2, but the currently-implemented OAuth2 flows are created for client applications where the user can be periodically prompted for credentials (or MFA) to obtain a new grant. As a server application, Venafi requires an unattended authentication method. We strongly recommend you configure your SMTP to use Secure TLS communication on a supported port. The Microsoft Exchange team's solution for continued support is using High Volume Email (HVE) for Microsoft 365, Azure Communication Services for Email, or an Exchange Server on-premises in a hybrid configuration. For instructions on how to onboard to High Volume Email for Microsoft 365, see instructions from Microsoft at https://learn.microsoft.com/en-us/Exchange/mail-flow-best-practices/high-volume-mails-m365. This solution uses port 587 and authenticates to Office 365 using a HVE account username and password.
Sender E-mail	This is the e-mail address the recipient will see in the "From" field of their email message.
Use Secure	This setting enables the email client and server to exchange messages using

Field	Description
TLS communication	the Transport Layer Security (TLS) protocol, which encrypts the data and verifies the identity of and integrity of the parties involved.
Log event for each delivered message	When checked, Venafi Configuration Console will log an event for every email message it sends. This feature is useful to meet some organization's auditing requirements.
Lock settings [...]	When checked, individual SMTP channels or Reporting modules will not be able to override these settings. This is analogous to locking the policy setting.
Authenticate to SMTP Server	This setting requires the email client to provide a valid user name and password to the SMTP server before it can send or receive email messages. When selected, the following two fields become available.
Username	The username used to authenticate the SMTP connection to the email host.
Password	The password used to authenticate the SMTP connection to the email host.
Send Test E-mail	Click to test the connection to ensure Venafi Platform can send messages using these settings.

6. Click **OK**.

IMPORTANT Until SMTP outbound server settings are configured for the first time, SMTP channels are disabled. Do not attempt to send any logs to SMTP channels until you configure SMTP outbound server settings as described above.

The first time you configure an SMTP connection, the built-in SMTP channels automatically become enabled.

6

Setting up notification channels

Channels provide the targets for where and how event logs are stored or transmitted to an external service. Channels are configured and managed in Venafi Configuration Console's **Tools** > **Logging** node.

Channels store the information the Venafi log server needs to deliver the log to the desired target. For example, MS SQL channel objects include the information needed to store messages in a database. SMTP channel objects include the information needed to send email messages with logged event information.

> **NOTE** Venafi Platform channels support both IPv4 and IPv6 connections.

This chapter contains the following topics:

Chapter 48: SQL Server channel requirements 444

Chapter 49: SQL Server channel configuration 445

Chapter 50: Updating the SQL Server channel object 448

Chapter 51: Creating a SQL Server log channel 448

Chapter 52: SMTP channel factory template upgrade considerations 451

Chapter 53: SMTP outbound server configuration 451

Chapter 54: Email templates 452

- Email Templates in VCC 452
- Customization and Upgrades 453

Flexibility in Configuration ... 453

Chapter 55: Managing logos and images used in email templates ... 453

Chapter 56: About SMTP templates for email notifications ... 456

Where to Find Templates ... 456

Customizing Templates ... 456

Setting the Default Template ... 456

Preservation During Upgrades ... 457

Resetting to Default Configuration ... 457

Chapter 57: Editing SMTP message templates ... 457

Using the Template Editor ... 458

Working with macros, images, and variables ... 458

Chapter 58: Built-in SMTP channels ... 460

SMTP channel properties ... 461

ChapterEditing SMTP channel message contents for email notifications 59: ... 465

Specify a template ... 465

Preview the message ... 465

Define variable values ... 465

Chapter 60: Message delivery failures ... 466

Chapter 61: Adaptable Log Channel prerequisites ... 467

What's next? 468

Chapter 62: About the Adaptable Log Channel PowerShell script 468

ChapterExample: creating a ServiceNow incident for expiring certificates 63: 471

Chapter 64: Configuring the Adaptable Log Channel object 472

ChapterProtecting against unapproved changes to Adaptable Log Channel 65: scripts 475

Chapter 66: PowerShell script reference for Adaptable Log Channel 476

About debug logging 477

Chapter 67: About hash tables 478

Chapter 68: Perform-Action function 478

Chapter 69: File channel requirements 483

Chapter 70: File channel configuration 483

Chapter 71: Filter channel configuration 487

What happens if I select items for both Events and Severity? 488

SNMP Versions and Compatibility 488

Management Information Base (MIB) 489

Customizing the MIB 489

Chapter 72: SNMP channel requirements 489

Chapter 73: SNMP Channel object configuration 490

Chapter 74: Customizing the Management Information Base 493

About the CEF format 495
About the JSON format 495
About the BSD format 496
About TLS 496
Chapter 75: Syslog channel prerequisites 496
Chapter 76: To configure a syslog channel object 497

About configuring the Channels folder

The Channels folder contains objects that manage communication between Trust Protection Platform and other external services and that are receive event logs and messages. The Channels folder stores:

- The Default SQL Channel, which is where all logs are stored by default.
- A folder of Built-in channels.
- Any additional folders and channels you create.

IMPORTANT E-mail notifications can only be sent if the **Log Channels** SMTP Default Connector is set up correctly. This is configured on the **Connectors** node in VCC. For detailed steps, see "Setting up SMTP settings for outbound email connections" on page 435.

Creating Channel objects

Trust Protection Platform is designed so you can create multiple channel instances for any given channel type. This means you can create multiple channel configurations to handle different functions or events. For instance, you can configure the Venafi Log server to use one MS SQL Channel object as the Default SQL Channel and another MS SQL Channel as a specialized log store for specific types of events.

You can also define multiple SMTP channel objects to send notifications to different recipients such as the contact for each application that consumes a given certificate, the certificate contact, the system administrator, and a certificate approver. Every SMTP channel object supports both plain text and HTML messages.

NOTE To view examples of channel object configurations, review the default channel objects that are provided in the **Channels** > **Built-In** node. You can use the default channels as-is, you can modify the default channels, or you can reference their configurations as a guide to help you create your own channel objects.

If you modify a default channel, you can revert it to it's factory settings at any time by clicking on the channel, then clicking the **Revert** action.

To create a channel object in VCC

1. In Venafi Configuration Console (VCC), browse to the **Tools** > **Logging** > **Channels** node.
2. In the **Actions** panel, click the type of channel you want to create.
    - **SQL Server**: Log events to a Microsoft SQL Server database. For more information, see "SQL Server channel" below.
    - **SMTP** Forward logged events to specified a specified email destination. For more information, see "SMTP channel" on page 450.
    - **Adaptable**: Log events to a custom channel. For more information, see Using Venafi's Adaptable Log Channel.
    - **File**: Log untranslated or translated events to a human-readable log file. For more information, see "File channel" on page 481.
    - **Filter:** Log events based on event type or severity to reduce the number of events logged to a database. For more information, see "Filter channel" on page 486.
    - **SNMP**: Forward logged events to an Simple Network Management (SNMP) system. For more information, see "SNMP Versions and Compatibility" on page 488.
    - **Syslog**: Forward logged events to a syslog server. For more information, see "About the CEF format" on page 495.
3. Complete the channel configuration, then click **OK**.

SQL Server channel

The SQL Server channel allows the Venafi log server to record events to a Microsoft SQL Server database. To store events, you can use the Trust Protection Platform database that you set up during installation or create a custom database.

IMPORTANT Venafi highly recommends stopping all Trust Protection Platform services prior to any scheduled database maintenance. Neglecting to so may produce unexpected behavior because Trust Protection Platform is dependent upon the database for the majority of its configuration and certificate data. Trust Protection Platform has been designed to handle brief loss of database connectivity due to network issues or similar anomalies but that should not be relied upon for extended database outages, especially those which are planned.

SQL Server channel requirements

Trust Protection Platform logs events to the location that is defined in the default channel. At installation time, the events log to the Trust Protection Platform database. However, if there are large volumes of events, you may want to consider creating a separate database and corresponding custom SQL Server channel just for processing log events.

As a general baseline, Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring. The space you need for your database depends on a number of factors. These include, but are not limited to, how many events per second you are storing and how long you want to keep the data.

IMPORTANT You must ensure the database server that stores the channel data does not run out of disk space. If the server runs out of disk space, the log server cannot operate.

The space you need for your log store depends on a number of factors that include, but are not limited to, how many events per second you are storing and how long you want to keep the data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.

WARNING! If you are using your Venafi server as your logging server, if your server runs out of disk space, the *entire set* of Venafi services on that server will stop working.

When using a separate MS SQL database, please refer to the Supported Databases section in the general System Requirements, as the specifications are the same.

For more information about Trust Protection Platform system requirements, see System requirements for Venafi components in the *Trust Protection Platform Installation Guide*.

SQL Server channel configuration

The SQL server channel stores information that the system needs to write events to an SQL Server database. During installation, Trust Protection Platform uses the database connection information to create the Default SQL Channel. This is the datastore where the Venafi log server logs all events.

For details on the SQL Server channel configuration, see "Updating the SQL Server channel object" on page 448.

Field	DSN Type	Description
Table	System, Custom	Specify which existing table in the connected database to use for the logs sent through this connector. This table must already exist.
Automatically delete...	System, Custom	Continually prunes log entries from the target database for logs older than the specified interval. We recommend you leave this setting enabled unless operational requirements (like legal data retention requirements) tell you otherwise. **IMPORTANT** It is very important that you properly manage log file size. If the server runs out of disk space, the log server cannot operate. If the database is on the same server as Venafi Platform and the server runs out of disk space, you will likely have a service outage. The size of your log store depends on a number of factors that include the number of generated events per second and the retention period for data. Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.
DSN	System, Custom	You can choose one of two database options: ■ Use system DSN. Use the same database that Venafi Platform is using.

Field	DSN Type	Description
		■ Custom Connection Data. Use a different database to store logs sent through this channel. **NOTE** The rest of the fields below are *only* displayed if you choose the Custom Connection Data option.
Username	Custom	The account name that the Log server uses to authenticate with the custom database. This account must have `db_datawriter` and `db_datareader` in the log store database. Requires additional grants. For more information, see "Creating a SQL Server log channel" on page 448.
Password	Custom	The password that the Log server uses to authenticate with the custom database.
Host	Custom	The IP address or hostname of the custom Microsoft SQL database server. Trust Protection Platform supports both IPv4 and IPv6 connections to MS SQL database servers. If a hostname is specified, only the first resolved address associated with that name is used.
Port	Custom	The port where the Log server connects to the custom database. For example 1433.
Database	Custom	The name of the custom database where the Log server writes events. This database must already exist. The SQL Server channel driver does not create the database.

Field	DSN Type	Description
Encrypt all database communications	Custom	Enabling this option encrypts all communications between the Trust Protection Platform server and the custom back end database. If this option is not selected, the credentials are still protected but all other communications between the server and the database might not be protected. Recommendation: Enable To learn how to enable SSL encryption for an instance of SQL server by using Microsoft Management Console, visit: https://support.microsoft.com/en-us/help/316898/how-to-enable-ssl-encryption-for-an-instance-of-sql-server-by-using-mi.
Windows Authentication	Custom	Windows Authentication will be used for the database connection. If you select this option, Log server authenticates to the database using a Windows user account and password instead of database credentials. Be sure to verify the following configurations: ■ All Log servers must use Windows Authentication credentials. ■ All Trust Protection Platform servers provide Windows Authentication for Policy Tree. ■ The Windows Authentication credentials have access to the database. When you select this option, the **Username** and **Password** fields, above, are disabled.
Enable "AlwaysOn Availability Groups" support	Custom	The Always On Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. For more information, see Always On Availability Groups (SQL Server).

Updating the SQL Server channel object

During installation, Trust Protection Platform automatically creates a database table and configures the default SQL Channel object to store log events in the table. The default SQL Channel object controls the location where the Log server stores event logs.

The default SQL Channel only requires configuration if you are using a separate database to store log events. A separate database for event logging requires you to create a custom SQL channel, and then change the default SQL channel object.

To update the default SQL channel object

1. Log in to Venafi Configuration Console (VCC) and browse to the **Tools** > **Logging** > **Channels** node.
2. Click **Default SQL Channel**, then click **Properties**.
3. Configure the other settings as described in "SQL Server channel configuration" on page 445.
4. Click **Save**.
5. Restart the Log service.

Creating a SQL Server log channel

When you're dealing with a high volume of log events, a custom SQL log channel can be helpful. By setting one up in the Venafi Configuration Console, you can direct events to an additional database you've created. This way, depending on your notification and policy settings, Venafi Platform will log events to either its own database or your new custom database.

Initial database setup

- **Create Database**: Open SQL Server Management Studio and create a new database.
- **Server Requirements**: If you're using a separate SQL Server for your custom log database, make sure it meets Venafi's database server requirements. For details, see System requirements for Venafi components.
- **High-Availability** (Optional): You can configure the SQL Server for high availability using Microsoft's Always On Availability Groups. For more information, see Always On Availability Groups (SQL Server).
- **Database Naming**: Database names must follow standard Venafi requirements.

  The database name cannot contain any of the following characters:

  ```
  [](){}\"',$%*?
  ```

Script Execution

1. Open script.

   Navigate to *[Venafi installation folder]\Database Scripts\MSSQL\Updates\Optional\mssql_log_structure_SP.sql*.

2. Run script.

   Run *mssql_log_structure_SP.sql* against the new database. This will generate additional stored procedures, tables, and types.

3. Create Log Channel.

   On the new database, run *DAL_LOG_SP_CREATE_LOG_CHANNEL 'table prefix'*. For example, *exec dbo.DAL_LOG_SP_CREATE_LOG_CHANNEL 'Log3'*.

4. Account Permissions. (Optional)

   If you're using an account other than `sa`, run the following set of grants listed below:

   - Open *[Venafi installation folder]\Database Scripts\MSSQL\Updates\Optional\mssql_log_grant.sql*.
   - Follow the instructions in the `mssql_log_grant.sql` file to grant permissions to an operational database account.

Configuration in Venafi Configuration Console (VCC)

1. Create SQL Server channel.

   In Venafi Configuration Console, expand the **Tools** > **Logging** > **Channels** nodes, then click **SQL Server** in the Actions panel, and give the new channel a name.

2. Configure the channel.
   - Specify the database **table** to use to store the logs.
   - Decide if you want to automatically delete records after a specified number of days.

     We strongly recommend you enable this option unless you have a specific operational requirement to maintain logs. If you don't purge log files regularly, your database can get very large, and if you log enough events, can even run out of storage space.
   - Choose **Custom Connection Data**.
   - Enter the database connection information.

Final steps

1. Create notification rules.

   You'll need to create the notification rules that will be stored to this database, and you will need to point them to your new custom SQL Server channel. For more information see "Working with notification rules" on page 501.

2. Restart log server.

   In VCC, go to the **Product** node, and click the **Logging** Windows service. In the **Actions** panel, click **Restart**.

SMTP channel

The SMTP channel delivers logging data to email through an SMTP server.

To send notifications using an SMTP channel, administrators can do any of the following:

- Use the built-in SMTP channels. These channels already have notification rules associated with them and will start working as soon as an outgoing SMTP server is configured.
- Edit the built-in SMTP channels. You can edit them directly, or duplicate them and modify the copies.

- Create new SMTP channels. You can configure notification rules to point to new SMTP channels you create. Once your new SMTP channels have been configured, see "Working with notification rules" on page 501.

SMTP channel factory template upgrade considerations

Venafi Platform offers a range of pre-configured SMTP channels for a wide variety of events. Feel free to use these channels as they are, tweak them to better fit your needs, or duplicate them to create customized channels.

Starting with Venafi Platform version 25.1, any changes you make to these default channels will stick around, even after system upgrades. Plus, you can always revert to the factory settings of any built-in channel whenever you like.

> **EXAMPLE** Consider the following scenario:
>
> Let's say you installed Venafi Platform version 25.1 and customized a default email channel to align with your company's requirements. When you later upgrade to version 24.1, your customizations will be preserved.
>
> So, what if Venafi updates that channel in a future release, like 25.1? No worries—your changes will still be there after the upgrade. If you ever want to go back to the factory settings, simply choose "Reset customization" from the VCC Actions menu. This will revert the channel to the most recent factory version—in this example, version 25.1.

SMTP outbound server configuration

SMTP channels need to communicate with an external SMTP server so logs can be delivered as email messages. The outbound SMTP server configuration is found in VCC in the **Connections** node.

For specific steps on adding SMTP server connection information so the SMTP channels can delver notifications, see "Setting up SMTP settings for outbound email connections" on page 435.

Until the outbound SMTP server settings are configured for the first time, SMTP channels are disabled. Venafi Platform automatically performs a one-time process to enable the SMTP channels as soon as the outbound SMTP server settings are first set up.

Email templates

Venafi Platform's SMTP channels are designed to send multi-part email messages, which include both HTML-formatted and plain-text content, to designated recipients.

Here's a quick refresher on how emails are generated in Venafi Platform

The log server watches for events that match notification rules. When an event matches a notification rule, the notification rule passes log information to a channel; in the case of email messages, it is an SMTP channel. The SMTP channel applies an email template, resolves the macros, inserts the log information, and sends the email to the desired recipient.

Email Templates in VCC

In Venafi Configuration Console (VCC), you'll find email templates that come with common formatting elements like logos, CSS styles, and message footers. These templates feature placeholders where the SMTP channel fills in the actual log content.

The beauty of these templates is that they centralize common elements. If you need to change a logo or tweak a style, you just update the template, and all SMTP channels using that template will automatically reflect the change.

The **Manage Templates** action is available in the Channels node and all its descendant nodes.

Customization and Upgrades

You're not limited to a single template; you can have multiple to suit your organization's diverse needs. If you decide to modify a factory template or built-in channel, those changes will stick around even after a server upgrade. And if you ever want to revert to the original settings, you can do so at any time.

Flexibility in Configuration

Feel free to edit built-in items directly or to copy existing templates and SMTP channels for quick modifications. You also have the option to create templates and SMTP channels from scratch, giving you maximum flexibility in how you manage your SMTP log delivery.

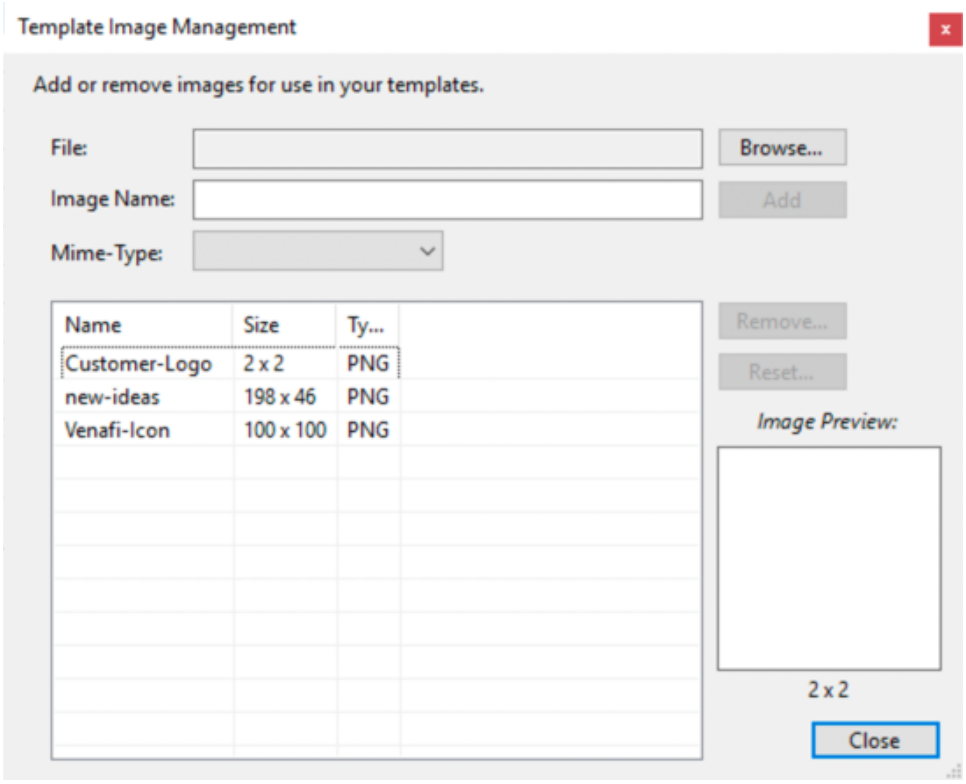
Managing logos and images used in email templates

Venafi Configuration Console (VCC) centralizes the management of images used in email templates. This makes it easy to add or remove images across all templates and messages where those images appear.

Before you start, ensure you have the images you want to use saved on the local system—either on the Venafi server for VCC or on your workstation if you're using the MMC snap-in.

To manage images for use in email notifications

1. In Venafi Configuration Console (VCC), go to **Tools** > **Channels**.
2. In the Actions panel, click **Manage Images** to open the Template Image Management window.



To add a new image:

1. Click **Browse** to locate the image file.
2. Click **Open**.
3. Verify the **Image Name** and the detected **Mime-Type**.

   The Image Name is what you'll use in templates, so make it short but descriptive.
4. Click **Add**.

To remove an image:

1. Select an image from the list.
2. Click **Remove** and then **Yes**.

If you remove a factory image and don't replace it, it will be restored the next time you refresh the Logging node.

To replace an image:

1. Select the image you want to replace and note the value in the **Name** column.
2. Click **Remove**.
3. Click **Browse** to locate the new image and click **Open**.
4. Replace the **Image Name** text with the value you noted earlier.
5. Verify the **Mime-Type** and click **Add**.

If you have replaced a Venafi-provided image, your change will be preserved when you upgrade Venafi Platform.

The factory image `Customer-Logo` is a transparent two-pixel square image that is pre-inserted in the default email template. If you replace this with your organization's logo, your logo will automatically appear at the top of the default message template. If you leave it as is, it won't cause any issues since it's transparent.

To reset a factory-provided image to its default state:

1. Select an image in the list.
2. Click **Reset**.

   The Reset option is only available for Venafi-provided images.

   You can't reset images not provided by Venafi. If the **Reset** button is disabled, the image you selected is not a Venafi-provided image.
3. Click **Yes**.

About SMTP templates for email notifications

Email templates in Venafi Platform serve as a wrapper for your message content, providing a consistent header, footer, style, and structure. The power of using templates is that a single change can update all messages based on that template.

Where to Find Templates

Templates are managed within the Venafi Configuration Console (VCC) under **Tools** > **Logging** > **Channels** or any of its descendants.

Customizing Templates

Venafi Platform comes with a built-in email template that serves as the default for all SMTP notifications. You have several options for customization:

- Edit the built-in template directly.
- Duplicate the built-in template and edit the copy.
- Create a new template from scratch.

For more information, see "Editing SMTP message templates" on the facing page.

Setting the Default Template

If you have multiple templates, you'll need to designate one as the default. This is the template that will be used when no other template is specified in the SMTP channel object.

Preservation During Upgrades

SMTP templates are safeguarded during system upgrades. Any changes you make will be retained when you upgrade to a newer version of Venafi Platform.

Resetting to Default Configuration

If you've modified the built-in template and wish to revert to the original settings, you can easily reset it to its out-of-box configuration.

Editing SMTP message templates

If you want to change the templates used to send SMTP messages, you'll need to go to the Venafi Configuration Console (VCC) (or use the Tools MMC snap-in).

To open the template editor

1. In VCC, go to **Tools** > **Logging** > **Channels**.
2. Click **Manage Templates** in the actions panel.
3. Do one of the following:
    - To modify an existing template, click its name, then click **Edit**.
    - To edit a copy of an existing template, click its name, click **Duplicate**, and then click **Edit**.
    - To create a new template from scratch, click **New**.

Using the Template Editor

The template editor is a robust tool for crafting both HTML-based and plain text message templates. Both versions of the message are sent to recipients; their email system determines which version of the message to display.

You can edit the template name and author in the bottom right corner of the Template Editor.

Working with macros, images, and variables

There are three types of dynamic content used in the Template Editor: Macros, images, and variables.

Macros

Macros are keyword-based commands enclosed by a single `$` symbol. They pull system information into notifications. For example, `$IdentityEmail[<PrefixedUniversal>]$` would insert the corresponding certificate owner's email.

Macros are available in the menu across the top of the Template Editor. Click **Documentation** to see reference documentation for the selected macro. (To hide the help window, click **Documentation** again.)

Images

Images are variables enclosed by three `$$$` symbols and are *always* the value of the `src=` attribute. For example: `<img src="$$$Venafi-Icon$$$" />`

To learn how to manage images, see "Managing logos and images used in email templates" on page 453

To insert an image into the message at the current position, click the logo title, then click **Insert Image Reference**.

Variables

Variables are units of dynamic content that will be replaced with specific content defined in the individual SMTP channel settings. When you have multiple templates, you'll see a couple of different groupings of variables. *Shared* variables are variables that exist in all templates. Conversely, *custom* variables only exist in a subset of templates.

When possible, we recommend you use shared variables as much as possible. Using shared variables makes your templates more useful because they can be used by emails that use any of the templates. If you use custom variables, you need to make sure the message settings in the SMTP channels match the variables of their templates.

In the Template Editor, you create and use variables by surrounding text with three `$$$` symbols. For example, this is a shared variable called title: `$$$Title$$$`.[1]

For example, if you have a detailed internal knowledge base, and you want to provide a link to different KB articles for different SMTP channels, you could create a variable called `$$$KbUrl$$$`. You could then define that URL for each SMTP channel in the Edit Message window. [2]

When you create variables, you can see them in the Detected Variables panel. On the right of the detected variable name you can see if the components were found in the HTML or Plain text versions of the message. To find the component's location in the email, click the name in the variable list, then click **Go to variable**.

One notable feature is the ability to nest variables. This means a variable can contain one or more other variables, allowing you to create reusable combinations of variables. If the system detects a recursive variable (a loop where a variable contains itself somewhere in the definition), it will output the loop five times, and will then stop generating. This helps you visually identify cases of recursive variables so you can hopefully fix them before the broken messages get sent to your users.

HTML and plain text messages

SMTP messages should be created in both the HTML and Plain text tabs. Depending on the recipient device and software, either the HTML or plain text version of the message may be shown to users. For example, if the SMTP channel target is a modern email system, the HTML version would likely be displayed. However, if the SMTP channel target is an SMS destination, the plain text version would be displayed.

In the HTML tab, you can use standard HTML syntax, including CSS in the style element, as well as inline CSS. The Preview window shows you a visual rendition of what the message will look like.

---

[1] The syntax for variables, macros, and images is CASE-SENSITIVE.
[2] Remember that you will need to specify this value on every SMTP channel that use this template. In this example of a country-specific URL, another reasonable approach would be to create separate templates for different regions, and just use the actual URL in the template code, so that you don't have to edit every SMTP channel to include the correct URL, and then assign the correct template to the correct SMTP channels.

Individual SMTP channels can be set to only deliver plain text versions, if needed. This is useful, for example, if the resulting email will be automatically processed by another system where a plain text version is preferable.

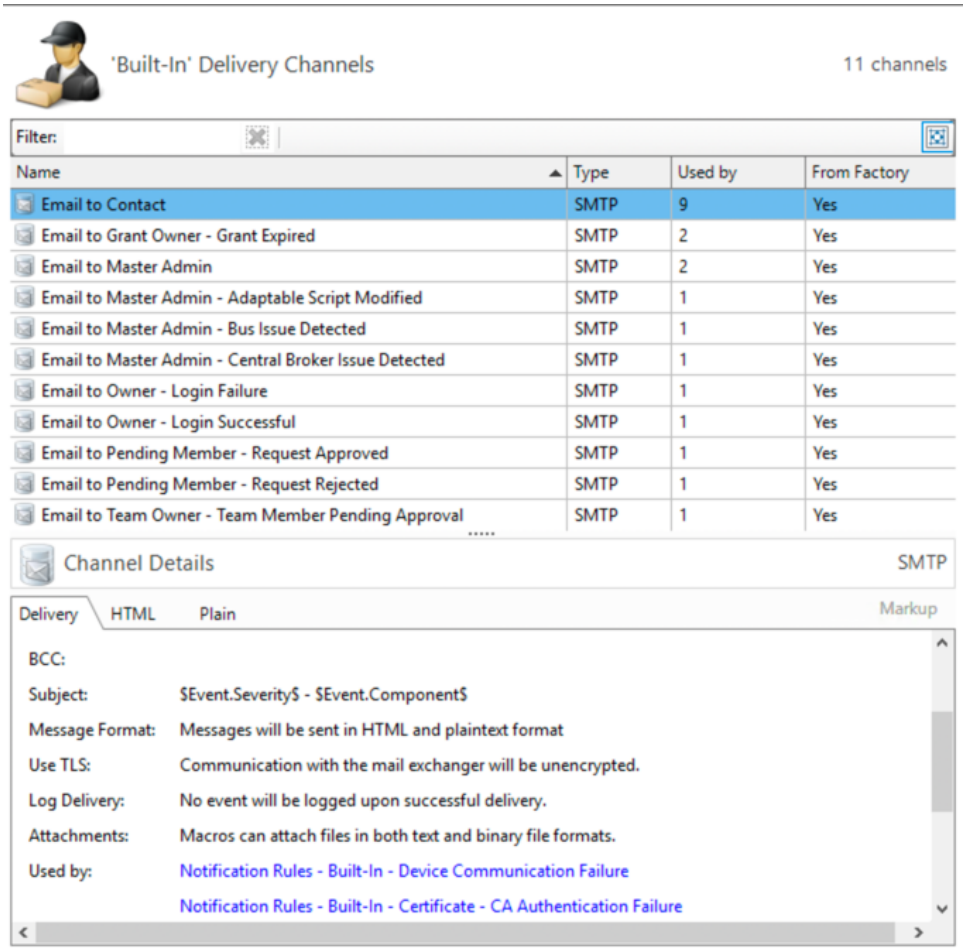
Saving your changes

Make sure you save your changes before you close the window. Once your changes are saved, all SMTP messages that use this template will be sent with the updated settings.

Built-in SMTP channels

The Channels node in Venafi Configuration Console (VCC) includes about 45 built-in channels, all but one of which are SMTP channels.

Expand the folders in the Channels node to see the sub channels. Notifications are grouped by product area.



The table shows the defined delivery channels in this folder. The bottom panel shows details about the channel settings. In the case of SMTP channels you can also see the HTML and plain-text renderings of the message.

The Delivery tab shows how the message will be delivered, the object configuration settings, as well a list of the notification rules that are connected to the channel.

For SMTP objects, the actions panel allows you to set the **Properties**, or you can click **Edit Message** to customize the contents of the notification.

SMTP channel properties

When you click the Properties action you can edit the settings that control how messages are sent. The following table shows the properties and their descriptions. Note that all text fields support macros.

SMTP Options

Field	Accepts Macros	Description
Description	No	A plain text description of the purpose of the SMTP channel.
Host	No	Hostname or IP address of the SMTP server. Trust Protection Platform Channel drivers support both IPv4 and IPv6 connections. If a hostname is specified, only the first resolved address associated with that name is used. You can append the port number to the host. For example: *<hostname>:25*.
Credential	No	Username credential required to authenticate with the SMTP server. Configure this option only if SMTP authentication is configured on your SMTP server. Otherwise, all notifications routed through this Channel object will fail.
Sender	Yes[1]	Name that appears in the From: line for all messages sent from this SMTP Channel object. Some SMTP servers require this field to be a valid email address. If this is required by your SMTP server, make sure you provide a valid email address, such as username@yourcompany.com.
Recipient	Yes	Specifies the recipients who should receive this notification. Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
CC	Yes	Specifies the recipients who should be copied on this notification. Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
BCC	Yes	Specifies the recipients who should receive a blind carbon copy of this notification. This field allows you to send the notification to a distribution list or group, but prevent "reply all" messages from being sent to the entire group.

[1]Use caution if you use a macro here, as it can lead to issues. For example, if the macro can't resolve, email messages may not get sent.

Field	Accepts Macros	Description
		Most commonly, this is a macro, such as $ConsumerEMail [$Event.Component$]$.
Subject	Yes	This will be the subject of the sent message.
Attachments	N/A	Some notification types can include files as attachments. Select **Allowed** to send attachments. Use the drop-down to specify the types of files that can be attached. If needed, you can ensure that items are not embedded, only attached. For example, a notification of a certificate renewal can include an attachment that contains the renewed certificate data.

Field	Accepts Macros	Description
Use TLS	N/A	Configures the SMTP channel driver to use Transport Layer Security (TLS) to send SMTP notifications. Select this option only if your SMTP server is configured to support TLS. Otherwise, all notifications routed through this Channel object will fail. SMTP channels can communicate with SMTP servers with or without authentication. SMTP channels can send events through servers that require SMTP authentication as long as a valid username credential is referenced in the SMTP channel configuration. If the username credential is configured, the SMTP channel *always* attempts SMTP authentication when connecting with the relay host. If the authentication failed, the SMTP driver logs an *SMTP Message Failure* event. If the SMTP channel successfully authenticates with the SMTP server and sends the message, it logs an *SMTP Message Success* event.
Log Delivery	N/A	The setting to manage SMTP events regarding delivery success or failure. *No*: Discard log events. *Yes*: Log email notifications. For example, the driver fails to connect to the SMTP server. If available, additional information appears in the exception details from the SMTP server. This information is helpful in troubleshooting connectivity and configuration issues.
Send Plaintext messages only	N/A	When *not* checked, messages are sent in both HTML and plain-text, and the client determines how to display the message. However, if you never want HTML messages sent to this channel, you can check this option.

Editing SMTP channel message contents for email notifications

The SMTP message editor in Venafi Configuration Console allows you to customize the value of the variables defined by the SMTP message template. It provides a list of variables on the left, and space on the right to define the variable value. You can insert macros into any variable value using the macros at the top of the page.

Specify a template

The **Use Template** drop-down allows you to choose **which template will be used to send the email** when you have multiple templates.

Preview the message

Click the **Show Preview** link to see a rendered version of the SMTP message.

At the top of the Message Preview window, you can select which template to use for the preview. You can also click the **View** button to switch between the HTML-based and plain-text renderings of the message.

Define variable values

For each variable in the list, you can specify the variable's value using any combination of text, HTML markup, and macro content.

Each variable name has an icon. Icons with a green check have a value defined for that variable. Icons with a red X *do not* have a value defined for that variable.

If a variable doesn't have a value defined, it will be excluded from the resulting message. For example, The `CallToAction` variable is displayed in the built-in email template as text in a `div` element on a colored background. If the variable value is empty, the `div` element itself is included in the message, but because it does not have any content it isn't visible.

Using macros in the SMTP Message Editor

Variable values can include text and macros. They can even include HTML markup. For example, the built-in channel *'Email to Pending Member - Request Rejected'* has the following default value for the `Details` variable:

```
<p><b>Rejection Comment:</b> $DictionaryKey[$Event.Data$, "Comment"]$</p>
<p><b>Rejected by:</b> $Identity[$Event.Text1$]$</p>
<p><b>Requested by:</b> $Identity[$DictionaryKey[$Event.Data$, "Suggested By"]$]$</p>
```

In this example, notice the combination of macros, text, and HTML markup.

> **NOTE** When HTML formatting is included in a variable's value, the markup is stripped out for plain-text messages.

To add a macro to a variable's value, use the Macro menu at the top of the editor. Use the **Documentation** button to learn more about the highlighted variable. (Use the **Documentation** button again to hide the help window.)

Use the **Toggle Word Wrap** button to make long variable values easier to read and edit.

When you are doing making changes, be sure to **Save** your changes.

Message delivery failures

If the SMTP channel driver can successfully send an event message, it logs an *SMTP Message Success* event. Otherwise, the SMTP channel driver logs a *SMTP Message Failure* event for the following reasons.

- Configuration errors in the SMTP Channel object. The SMTP channel driver does not buffer events that are undeliverable because of a misconfiguration.
- Connect issues with the SMTP server. To help you troubleshoot the message failure, SMTP Message Failure events provide the exception details returned from the SMTP server.

Adaptable Log channel

The Adaptable Log Channel driver lets you implement custom actions in response to events that are logged by Trust Protection Platform.

This driver can perform virtually any programmatic task in response to the logging of an event. The Adaptable Log Channel driver can interface directly with ITSM and/or SIEM solutions to create support tickets, change requests, security incidents, and so forth.

For applications that require access to the Venafi Web SDK, Trust Protection Platform can manage authentication for you automatically, reducing the overhead in your PowerShell script. When implemented, each time your script is called, Trust Protection Platform requests a new token automatically. Each new token is associated with both the specified user and with the referenced application ID. After the script finishes running, Trust Protection Platform revokes the token automatically. To get started, see "Adaptable Log Channel prerequisites" below.

Adaptable Log Channel prerequisites

Before you configure a Venafi Adaptable Driver object in Trust Protection Platform, review the following prerequisites:

- Review the Adaptable Log Channel design to determine the Trust Protection Platform logged events to which you want the driver to respond.
- To work effectively with any Venafi adaptable solution, you must have some working knowledge of PowerShell scripting, or you must have equivalent experience with a scripting language similar to PowerShell.

- Identify who will write the logic for the PowerShell functions in the Adaptable Application driver script.

  Will you write the logic yourself, or will you delegate the task to an internal development resource, Venafi Professional Services, or someone else?

- Install Windows PowerShell 3.0 or later.
- Install .NET 4.8 or later.

What's next?

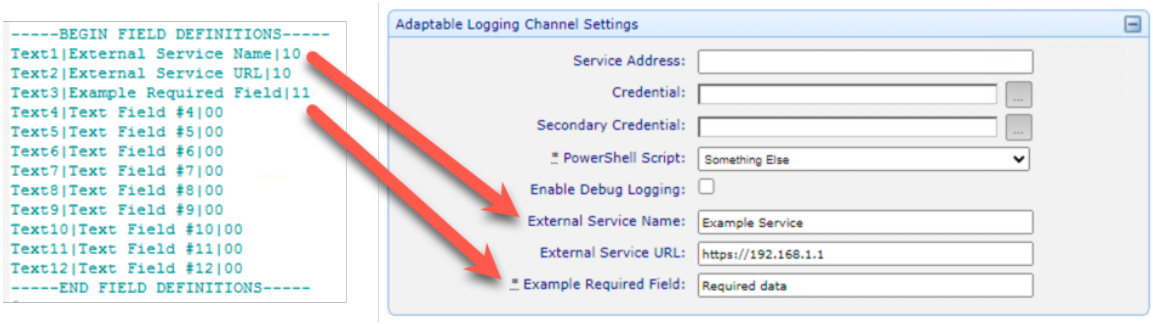
After you've completed the Adaptable Log Channel prerequisites, see "Configuring the Adaptable Log Channel object" on page 472.

About the Adaptable Log Channel PowerShell script

The Venafi Adaptable Log Channel, like the other Venafi Adaptable Drivers, uses PowerShell scripts that contain functions that can be used to perform virtually any programmatic task in response to a logged Venafi Platform event.

> **TIP** When creating new PowerShell scripts for use with adaptable drivers, keep in mind that the file name is used to identify your script from within the associated object (and within the policy for the Adaptable Application driver) in Trust Protection Platform. Using logical names can help you and other administrators recognize the purpose and intent of each script.

The Adaptable Log Channel configuration provides a common set of variables for use in Logging. However, if you need to pass unique or additional data to your script or third-party application, you can define up to twelve additional text fields. You do this by simply modifying the **Begin Field Definitions** section of the Adaptable Log Channel PowerShell script.



NOTE About macros: It's important to note that the Service Address field **does not accept macros**. You must use a custom field instead. Please be aware that certain macros are designed to function exclusively within workflows. Use the Macro Evaluator along with sample data to help you understand how macros will be processed for your use case.

Each field definition has three parts:

Field Name| *Field Label*| *Flags*

1. Field Name: Must be `Text1` through `Text12`. Do not modify these values.
2. Field Label: Type the name that you want to appear on the Adaptable Log Channel application object settings page.
3. Flags: Using the numeric values of `0` (to mean false) or `1` (to mean true) for each of the following options (in order):
    - Enabled: Use to enable or disable a field.
    - Mandatory: Use to indicate whether the field must be completed, or is optional. When set to true, this option adds an asterisk (*) next to the field label to let the user know that it is a required field.

EXAMPLE Suppose you want to add two required fields to capture an external logging application name and URL. Using a text (or PowerShell script) editor, you would open your PowerShell script file (which must be in the `[drive]:\\Venafi\Scripts\AdaptableLog\` folder). You would then edit the field definitions in the header section to include new fields like in the example below, then set and set values for the available flags:

```
----------BEGIN FIELD DEFINITIONS--------
Text1|External Log Provider Name|11
Text2|External Log Provider URL|11
Text3|Text3|00
Text4|Text4|00
Text5|Text5|00
Text6|Text6|00
Text7|Text7|00
Text8|Text8|00
Text9|Text9|00
Text10|Text10|00
Text11|Text11|00
Text12|Text12|00
```

When you are finished, you save your changes to the PowerShell script. When you open Policy Tree, your new fields appear on the Adaptable Log Channel objects.

IMPORTANT The header is required! The Powershell script will not work if the following header information is removed:

```
---- BEGIN FIELD DEFINITIONS ----
```

To create (or edit) Adaptable Log Channel data fields

1. Open your Adaptable Log Channel PowerShell file using a text (or PowerShell script) editor.

   Adaptable Log Channel PowerShell script files must be stored in the `\Venafi\Scripts\AdaptableLog\` folder.

2. Locate the **Begin Field Definitions** section and determine where you want to place your new field.

3. On the line where you want to define your new field, type the new field label and then set the appropriate flags.

   For example:

```
Text1|External Log Provider Name|11
Text2|External Log Provider URL|11
```

4. When you are finished, save the file and close it.

Your new field should appear on both the Adaptable Log Channel object page in Policy Tree as well as on the adaptable channel object in Venafi Configuration Console (VCC).

Example: creating a ServiceNow incident for expiring certificates

The Adaptable Log Channel driver lets you implement a custom action in response to events that are logged by Trust Protection Platform. The following sample code demonstrates calling the ServiceNow API to create an incident when a certificate is nearing expiration.

This sample script assumes that the Adaptable Log Channel object to which this script is assigned is targeted by a notification rule that executes whenever the *Certificate Monitor - Certificate Expiration Notice* and/or the *Certificate Monitor - Certificate Expiration Escalation Notice* events are logged.

```
function Perform-Action
 {
  Param(
   [Parameter(Mandatory=$true,HelpMessage="General Parameters")]
   [System.Collections.Hashtable]$General,
   [Parameter(Mandatory=$true,HelpMessage="Event Detail Parameters")]
   [System.Collections.Hashtable]$Event,
   [Parameter(Mandatory=$true,HelpMessage="Extra Field Parameters")]
   [System.Collections.Hashtable]$Fields
  )
  $passwd = ConvertTo-SecureString $General.UserPass -AsPlainText -Force
  $cred = New-Object System.Management.Automation.PSCredential($General.UserName, $passwd)
  $url = $General.ServiceAddress + "/api/now/table/incident"
  $body = @{
   "category"="request";
```

```
    "short_description"=$Fields.Text1;
    "description"=$Event.Description;
    "comments"="Created by Venafi Trust Protection Platform Adaptable Log Channel using the ServiceNow API";
    "impact"=3;
    "urgency"=3;
    "work_notes"=$Fields.Text2;
    "priority"=3; # 1=critical, 2=high, 3=moderate, 4=low, 5=planning
    "contact_type"="self-service";
    "caller_id"="68f87b0bdb97a2009dfaf91ebf9619e9"
  } | ConvertTo-Json
    $resp = Invoke-RestMethod -Uri $url -Credential $cred -Method Post -Body $body -ContentType "application/json"
    $sys_id = $resp.result.sys_id
    return @{ Result="Success"; Updates=@{"Description"="ServiceNow Incident ID=" + $sys_id} }
}
```

For another example of simplifying authentication to the Web SDK, take a look at this Venafi Cool Solutions article.

Configuring the Adaptable Log Channel object

Creating and configuring an Adaptable Log Channel object is similar to creating any other application object, except that you must specify the PowerShell script you want to use. However, in the case of Adaptable Log you can also make these configuration settings in Venafi Configuration Console or in the Tools MMC snap-in.

> **NOTE** Before you attempt to create CA template, device, or application objects, you must enable the *create* permission under the folder where you want to create the new object. For more information, see "Permissions overview" on page 713 in the *Administration Guide*.

To create and configure a new Adaptable Log Channel object

1. In Venafi Configuration Console (VCC) browse to the **Tools** > **Logging** > **Channels** node.
2. In the Add Channels section of the Actions panel, click **Adaptable**.
3. Provide the name you want to use for the new Adaptable Log channel, then click **Add**.

4. In the channel settings, configure the following:

   a. In the **Service Address** field, type the network address (e.g. URL) of the service with which the Adaptable Log Channel driver will interact.

   b. Click **Credential** to browse for the location of the credential object that you want to use to authenticate.

   > **NOTE** If you're connecting to the Venafi Web SDK, leave this field empty since you'll be specifying a credential in the WebSDK OAuth Token Configuration settings.

   Credential objects store the credentials Trust Protection Platform uses to authenticate with devices, applications, and CAs. The stored credential may be a password, a user name and password, a certificate, or a private key.

   > **NOTE** The user account you select must have *Read* and *Write* access to the Temporary, Private Key, and Certificate directories.
   >
   > For more information, see "Working with system credentials" on page 909the Managing system credentials section of the *Venafi Trust Protection Platform Administration Guide*.

   c. (Optional) (Conditional) If you need to select another credential, then from the **Secondary Credential** field, select a username, certificate, password, or CyberArk credential object.

   > **TIP** Use this option to avoid having to hard code additional credentials in your script or having to utilize other solutions outside of Trust Protection Platform.

   d. From the **PowerShell Script** list, select your custom PowerShell script.

   Your custom scripts must be in the `\Venafi\Scripts\AdaptableLog\` folder in order to appear in this list.

   > **BEST PRACTICE** You should consider placing Adaptable scripts on all of your Trust Protection Platform servers so that you don't have to worry about the roles those servers are performing.
   >
   > Adaptable Log Channel scripts *must* be placed on both the server that's hosting the Venafi web-based console, and any other servers where you're running Venafi's Log servers. For both the Adaptable CA and Adaptable Application drivers, PowerShell scripts *must* be placed on the Venafi server that hosts Policy Tree, as well as on processing engines that are used for enrolling or provisioning work.
   >
   > For an explanation of the various Trust Protection Platform administration consoles, see "About Venafi Trust Protection Platform administration consoles" on page 3.

e. (Optional) If you want to enhance troubleshooting capabilities of your Adaptable Log ChannelAdaptable Flow, select the **Enable Debug Logging** check box.

For information about how enabling this option works with the PowerShell script, see "About debug logging" on page 477 in the Adaptable Log Channel Adaptable Flow PowerShell script reference.

5. (Optional) If your application will connect to the Venafi Web SDK, then complete the **WebSDK OAuth Token Configuration** settings:

Setting	Description
OAuth Token Application ID	Enter the application ID of the *API application integration* you should have created previously, as described in "Adaptable Log Channel prerequisites" on page 467.
OAuth Token Credential	Select the username credential of the service account that has been granted access to the Client ID of the API Application. See "Adaptable Log Channel prerequisites" on page 467. In this context, the username credential identifies the user (identity) for whom the token is being requested. It also verifies whether you have the required permissions within your organization to enable the script to authenticate as the selected user. This security measure prevents users from impersonating another user.
OAuth Token Scope	(Optional) Enter one or more of the scopes assigned to your API application. For example, Certificates: Manage. Leave this field blank if you want to include all defined scopes. To learn more about scopes and restrictions, see Token Auth scope in the Developer's Guide.

NOTE If your application is not connecting to the Web SDK, leave all of these fields blank.

6. (Conditional) If your script includes customized fields, enter the desired static text or macro commands.

Refer to the sample in the topic, "Example: creating a ServiceNow incident for expiring certificates" on page 471.

For more information about Venafi's macros, see Macro commands in the *Macro Guide*.

7. When you're finished, click **OK**.

IMPORTANT If you make changes to the PowerShell script used by an Adaptable Log Channel, you must open the corresponding log channel object and click **Save** to force the driver to re-read the script, which will happen almost instantly.

Protecting against unapproved changes to Adaptable Log Channel scripts

Venafi's Adaptable drivers—such as Adaptable CA, Adaptable Application, Adaptable Bulk Provisioning, and Adaptable Log Channel—rely on PowerShell scripts stored in the *\Venafi\Scripts\AdaptableDriverName* directory on Trust Protection Platform servers. To ensure the integrity of these scripts, Trust Protection Platform supports signed scripts.

Because other people might have access to the server that is running Trust Protection Platform, they could modify your PowerShell scripts without your knowledge, either accidentally or intentionally. However, with signed scripts, any modifications made to the script will result in a failed signature validation, and the script will not be executed.

To protect against unapproved changes to your scripts, Trust Protection Platform monitors PowerShell script files that are being used by existing Adaptable objects. If a new script is used or a PowerShell script is modified on the file system, Trust Protection Platform displays a warning and you'll need to re-validate the script.

This security feature helps to prevent potentially harmful modifications to your scripts from being run.

IMPORTANT Because of this security feature, following an upgrade to Trust Protection Platform, you must take specific steps on all existing Adaptable objects in order for them to be re-enabled. Refer to the documentation for each Adaptable driver for details.

To use VCC to re-enable an Adaptable Log Channel driver after a script change

1. From Venafi Configuration Console (VCC), navigate to the **Tools** > **Logging** > **Channels** node.
2. Locate the adaptable log channel whose script was modified.
3. In the **Actions** panel, click **Properties**.
4. Click **Save**.

To use the web console to re-enable an Adaptable Log Channel driver after a script change

1. From the Platform menu bar, click Policy Tree.
2. From the **Tree** drop-down menu, select the **Logging** tree.
3. Expand the **Channels** folder and click your existing **Adaptable Log Channel**.
4. On the **Adaptable Channel** > **Settings** tab, click **Save**.

PowerShell script reference for Adaptable Log Channel

This section documents all available PowerShell functions for use with the Adaptable Log Server driver. PowerShell scripts are stored in the \Venafi\Scripts\AdaptableLog folder.

The input parameters and response format for each function is predefined. All functions receive a set of general parameters, whereas those parameters that are *specific* to the function are only passed to it.

> **DID YOU KNOW?** To prevent vulnerabilities, the PowerShell scripts are stored on the Trust Protection Platform server. While it might have been more convenient to allow downloading the script, storing the scripts on the Trust Protection Platform server prevents potentially harmful scripts from affecting the server. Only privileged users on your Trust Protection Platform server can access scripts.

You must ensure the same version of all your Adaptable Log Server scripts are on all servers in the cluster that have the WebConsole component installed. For this reason, it is wise to include a script version number in the file name, so you can easily check to see that the same version of the script is installed on all servers in the cluster.

NOTE To work effectively with any Venafi adaptable solution, you must have some working knowledge of PowerShell scripting, or you must have equivalent experience with a scripting language similar to PowerShell.

A sample script is provided in the `\Venafi\Scripts\AdaptableLog\Samples` folder. Only files that are in the main `\Venafi\Scripts\AdaptableSSHManagement\` folder can be selected in an Adaptable Log object in Policy Tree or VCC. Files in all sub-folders are ignored.

BEST PRACTICE When customizing (or creating a new) PowerShell script, keep the following security best practices in mind:

- Avoid hard-coding credentials into your PowerShell scripts.
- Only include code in functions that relate to the task they are designated to perform.
- Scripts should not do anything that could alter the integrity or availability of the local Windows system (the system hosting Trust Protection Platform).

IMPORTANT If you make changes to the PowerShell script used by an Adaptable Log Channel, you must open the corresponding log channel object and click **Save** to force the driver to re-read the script, which will happen almost instantly.

About debug logging

When a user has requested debug logging by checking **Enable Debug Logging** for Adaptable Log Channel, the driver sets a global variable called $DEBUG_FILE whenever it executes a PowerShell function. So your PowerShell script should reference the value of the $DEBUG_FILE variable to decide whether or not to log information for troubleshooting purposes. The value the driver assigns to the $DEBUG_FILE variable is a recommended file path name on the Trust Protection Platform server for use when logging events to a file. The file name is designed to be unique to the instance of the Adaptable component so as to avoid conflicts when multiple scripts are running at the same time and writing to the log file. If the recommended file name is used, the resulting log file appears in the `<Venafi Home>\Logs` directory by default (e.g. `C:\Program Files\Venafi\Logs`).

For information about where Enable Debug Logging is configured for Adaptable Log Channel, see "Configuring the Adaptable Log Channel object" on page 472.

About hash tables

Data is passed to (and returned by) each function using hash table data structures.

A *general* hash table, which includes a common set of data, is passed to available functions. A *specific* hash table, which includes data that is applicable specifically to the function, is passed to functions that require additional data. All functions must return a single hash table that includes a *result* along with any other variables that the function is required to return.

CAUTION Functions must not return errors; rather, they must throw exceptions in the same way that actual PowerShell errors do. The Adaptable Log Channel driver treats exceptions thrown by a PowerShell function as a fatal error and then halts processing.

Perform-Action function

Use the *Perform-Action* function to perform a specific action in response to the logging of an event by Trust Protection Platform.

Variable Name	Data Type	Description
AuxPass	String	The password portion of the Secondary Credential when a user name or a password credential is assigned, or the PKCS#12 password when a certificate credential is assigned
AuxPfxData	Byte Array	A PKCS#12 byte array that contains a client certificate and private key when a certificate credential is assigned as the Secondary Credential
AuxUser	String	The user name portion of the Secondary Credential when a user name credential is assigned
OAuthAccessToken	String	OAuth token passed to the PowerShell script. Tokens are passed only after you've provided the required information in the *WebSDK OAuth Token Configuration* settings of the Adaptable object. See "Configuring the Adaptable Log Channel object" on page 472. **How it works** When used, each time your script is called, Trust Protection Platform requests a new token automatically. Each new token is associated with both the specified user and with the referenced application ID. After the script finishes running, Trust Protection Platform revokes the token automatically. To get started, see "Adaptable Log Channel prerequisites" on page 467.
	String	The network address (e.g. URL) of the service with which the Adaptable Log Channel driver interacts.
UserName	String	The user name portion of the user name credential assigned to the Adaptable Log Channel instance. Used to authenticate with a remote system or service.
UserPass	String	The password portion of the user name credential assigned to the Adaptable Log Channel instance. Used to authenticate with a remote system or service.

Variable Name	Data Type	Description
ID	String	The event's Event ID field as defined in the logging application LSC file.
Name	String	The event's Description field as defined in the logging application LSC file.
Description	String	The event's Readable Log Text field as defined in the logging application Log Schema Channel (LSC) file.
Severity	Integer	The event's log level: ■ 1 = Emergency ■ 2 = Alert ■ 3 = Critical ■ 4 = Error ■ 5 = Warning ■ 6 = Notice ■ 7 = Info ■ 8 = Debug For more information, see About logging thresholds in the Log Server Administration Guide.
ServerDate	DateTime	The month, day, year, hour, minute, second, and millisecond (UTC) that the logging server received the event. The date and time displayed are specific to the Locale defined on the Log server.
ClientDate	DateTime	The date and time (UTC) that the logging application generated the event.
Component	String	The DN of the object–i.e., the application, CA, certificate, workflow ticket, device, or credential–that triggered the event.
Grouping	Integer	An ID that can be used to identify related events.
Text1	String	The value of this field depends upon the event. It can contain any text string up to 255 characters.

Variable Name	Data Type	Description
Text2	String	The value of this field depends upon the event. It can contain any text string up to 255 characters.
Value1	Integer	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
Value2	Integer	The value of this field depends upon the event. It can contain any numeric value up to 32 bits.
Data	ByteArray	The value of this field depends upon the event. The maximum data size is 1536 bytes.

Variable Name	Data Type	Description
Text1 *through* Text12	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.

Return	Data Type	Description
Result	String	Shows "Success" to indicate the non-error completion state.
Updates	String	(Optional) Hash table of attribute name-value pairs pertaining to the Event.Component that specify what the driver will update when the result is "Success."

File channel

The File channel collects log server events directly to a file in either the CSV format or the translated format (default setting), which writes the log in a human-readable format. The log data is defined in the corresponding event definition.

CSV files simply contain the event data; consequently, they are difficult to decipher. However, because these comma-delimited files maintain a consistent field structure across events, you can import these files into spreadsheet programs like Microsoft Excel to query the log data.

The following is a sample from a CSV log file:

```
2130706433,1250570028,1250570028,\VED\Engines\Jupiter,917507,Info,0,\VED\Engines\Jupiter\
TLS Protect,,0,0,,
 2130706433,1250570029,1250570029,\VED\Engines\Jupiter\TLS Protect,1245202,Info,0,,,10000,0,,
```

```
2130706433,1250570029,1250570029,\VED\Engines\Jupiter\TLS Protect
,1245197,Info,0,\VED\Policy\Import\cert1.venafi.com,10/05/2009 03:49:24,0,0,,
```

On the other hand, translated log files are more human-friendly. They can be visually scanned for content. However, it is difficult to generate reports from translated log files because there is no delimited field structure. They get their main content from the Translation field in the event definition. (In the event definition table view, this field is just called Log.)

The following is a sample from a translated log file:

```
127.0.0.1, 17/08/2024 22:17:41: EncryptionDPAPI initialized successfully.
127.0.0.1, 17/08/2024 22:17:42: The Venafi Encryption Trust Protection Platform service manager for the engine Jupiter is running in 32 bit mode.
127.0.0.1, 17/08/2024 22:17:42: The engine \VED\Engines\Jupiter is loading the service module \VED\Engines\Jupiter\TLS Protect.
127.0.0.1, 17/08/2024 22:17:42: The certificate management service module for the engine Jupiter is examining certificates for expiration.
127.0.0.1, 17/08/2024 22:17:42: The certificate management service module for the engine Jupiter is examining certificates for notification.
127.0.0.1, 17/08/2024 22:17:42: The certificate manager for Jupiter has found 10000 certificates for renewal expiration consideration.
127.0.0.1, 17/08/2024 22:17:42: The certificate manager for Jupiter has found 0 work to do requests for consideration.
```

The Venafi Log server can use the file channel to create specialized log files for specific types of events.

WARNING! If you are using a file channel, you should strongly consider only using a *single* log server. If you are using multiple log servers, and if your file output is saved locally on each Venafi server, you will have incomplete logs on each server. You would need to manually combine all log files for an accurate, complete log. If your file output is saved on a shared network drive, your log servers will constantly be competing to write to the file, which will result in errors and incomplete logs.

File channel requirements

The following list contains the requirements for file channels:

- To enable the Venafi Log server to log data to file, you must create and configure the File channel object in Trust Protection Platform. For information on creating the File channel object, see "Creating Channel objects" on page 442.
- The Log server must have full permissions to the log file directory defined in the File channel object.
- The space you need for your log file depends on a number of factors. These include, but are not limited to, how many events per second you are storing and how long you want to keep the data. As a general baseline, Trust Protection Platform generates about 10 events per certificate renewal. Daily events include validation checks and certificate monitoring.

File channel configuration

As described previously, the File channel uses the event definitions to create CSV and translated log files. Depending on the channel settings, the file will be written in CSV format, or in the translated, human-friendly format. The event definitions contain the all the data used for the resulting logs which will be stored, in the case of File channels, to a text file. When you create a file channel, you can choose whether the data in the file will be written in CSV format.

To manage resources, a File channel accumulates data and writes it periodically, so there may be a short delay between the event and the target log file being updated.

You should figure out how you will ensure the target disk doesn't get too full. If the disk runs out of space, the log server can *not* operate. The amount of disk space you need depends on a number of factors such as the retention period and the volume of events. For example, daily validation checks and certificate monitoring generate many event log entries. A certificate renewal can generate about 10 events.

To configure a File channel

1. In Venafi Configuration Console (VCC), open **Tools** > **Logging** > **Channels** .
2. If the File channel already exists, locate it and click the **Properties** action.

   If you need to create a new File channel, click **File...** in the **Add Channel** section of the **Actions** panel, then give the channel a name.
3. Use the following table to configure the File channel .

Field	Description
Path/File	The directory and/or filename of the File channel log. Periodically the File channel driver saves the data to the log file. The event log name and location depends on one or more of the following factors: ◦ If no value is provided, the log file is written in the default log directory, and the file name will match the File channel name. For example, *\Program Files\Venafi\Logs\MyFileChannelForEvents.log*. ◦ If the value contains the path, but omits the file name, the file name will match the File channel name, and will be written in the specified location. For example, *MyFileChannelForEvents.log*. ◦ If the value omits the file extension, the File channel automatically appends *.log* to the filename. ◦ If the value has a valid directory and filename, the File channel records the event data in the Trust Protection Platform server file system at the specified location. ◦ If the specified directory does not exist in the file system, Trust Protection Platform creates the folder and log file.
Options > Translate raw events into text	A setting to control the way the File channel records events: ◦ When checked: Record translated events in the UTF-8 format. Include a byte marker at the beginning of the log file. Record only the event description based on the Event ID and matching Translation field from the event definition. Not suitable for reporting because the data uses an inconsistent field structure. ◦ When cleared: Use CSV to store untranslated log files. Omit the byte marker. Show only raw event data in a comma separated format. Suitable for reporting. Record untranslated events in this format: *SourceIP,ClientTime,ServerTime,Component,ID,Severity,Grouping,Text1,Text2,Value1,Value2,MIMEType,Data*

Field	Description
Create new log file at midnight	A setting to control log file size based on log date. ◦ When checked: At midnight, the previous day's data is saved to another file with the date and time appended. If that filename already exists (which could happen if the *Create new file when size reaches xx MB* option is also checked), a new file is created with a unique trailing numeric digit. New logs will continue to be written to the specified log file name. ◦ When cleared: The system doesn't use the current date to determine if a new log file should be created.
Create new file when size reaches *xx* MiB[1]	A setting to control the log file size based on file size. ◦ When checked: When the specified log file reaches the maximum size, the data is saved to another file with the date and time appended. New logs will continue to be written to the specified log file name. ◦ When cleared: The system doesn't use log file size to determine if a new log file should be created.
Delete existing log files older than *xx* days	A setting to purge old event log files. This is an important part of managing log files so they don't exceed the space available on the server. ◦ When checked: Any log files that match the *Path/File* setting above will be deleted if it is older than the specified number of days. If errors occur during the purge, the File channel driver records the events to the Windows application log. ◦ When unchecked: The system doesn't automatically delete logs. You will need another way to manage storage space on the log server.

4. Click **OK**.

Filter channel

The Filter channel allows the Venafi log server to block certain events or severity levels from being passed to other channels. This is primarily used for the default channel as a way to prevent unhelpful amounts of logging.

[1]This value is represented in mebibytes, which represents 2^20 bytes, or 1.049 megabytes.

To implement a Filter channel, you must configure the Filter channel as an intermediary channel between the event source and the final output channel. It is configured in Venafi Configuration Console (VCC).

To filter the default channel

1. In VCC, open **Tools** > **Logging** > **Channels**.
2. Create the Filter channel.
3. Configure the Filter channel's **Target Channel** attribute to point to the default log channel (this is usually the Default SQL Server channel).
4. Open the **Tools** > **Logging** > **Servers** node.
5. Click the log server, then click **Properties**.
6. In the **Default Channel** setting, specify your new Filter channel.
7. If you have multiple log servers, repeat the previous two steps for all logging servers. It's important that all log servers use the same default channel settings.

   For more information on the Log server configuration, see "Managing the log server" on page 429.
8. Open the **Product** node in VCC and **Restart** the **Logging** service.

Filter channel configuration

The Filter channel stores the information the system needs to block designated events or severity levels.

The following table describes the configuration settings for Filter channels:

Field	Description
Forward to	Specify the target channel that the Filter channel passes the unfiltered events to after it filters out the blocked events or severity levels.
Filter	Use as a text search to locate specific events.
Events	Event Filter options allow you to select which events you want to **block**.

Field	Description
	Checked events will be displayed below the Events selection box. These events will not be passed along to the target channel.
Severity	Severity Filter options allow you to select which event severity levels you want to **block**. Any events matching the selected severity settings will be blocked and will not be passed along to the target channel. For more info on severity levels, see "Event IDs and severity levels" on page 424.

TIP If you need to select a large number of events, or even whole groups of events to block, you may prefer to edit the filter object in web console. From the TLS Protect menu, click **Logs**, then locate the Filter channel you want to modify. Then click inside the **Events Blocked** panel.

The **Event Selector** window allows you to bulk select events. Items in the **Available** list are events that are *not blocked*. Items in the **Selected** list *are blocked*, and will appear as checked items in the VCC Filter channel editor.

What happens if I select items for both Events and Severity?

If you specify settings for both events and severity level(s), events that match *either* setting will be blocked and will not be passed along to the target channel.

SNMP channel

The Simple Network Management Protocol (SNMP) is a widely-used protocol designed for network management. It allows for the collection and organization of information about managed devices on IP networks, as well as for modifying that information to change device behavior. SNMP is commonly used in a variety of settings including corporate networks, service provider networks, and many others. It serves as a critical tool for network administrators to manage network performance, find and solve network issues, and plan for network growth.

In the context of Venafi Platform, the SNMP channel enables the logging server to send traps—essentially alert messages—that contain specific event data to an SNMP management system. This integration allows for real-time monitoring and automated responses to specific conditions in your encryption environment.

SNMP Versions and Compatibility

Venafi Platform supports three versions of SNMP:

- **SNMP v1:** The original version, which only supports IPv4 connections.
- **SNMP v2c:** An extension of SNMP v1, supporting IPv4, IPv6, or dual-stack configurations.
- **SNMP v3:** The most secure version, also supporting IPv4, IPv6, or dual-stack configurations.

Management Information Base (MIB)

For SNMP v2c and v3, Venafi Platform employs its own Management Information Base (MIB) file. An MIB is essentially a database that defines the properties of the managed object within the network that can be accessed via SNMP. In this case, the MIB file maps events to specific Object IDs (OIDs). These OIDs include both the event fields and readable log text, simplifying the task of searching for specific traps in your SNMP monitoring system.

Customizing the MIB

If you add, delete, or modify events, the MIB file will need to be regenerated to reflect these changes. Administrators also have the option to customize the MIB file by altering the Venafi Platform event schema. For more in-depth information, consult the section on "Customizing the Management Information Base" on page 493.

SNMP channel requirements

For proper communication between the Venafi Log Server service and the Simple Network Management Protocol (SNMP) host, you should consider the following requirements:

- You must have the Read Write permission to the Log Application objects.
- Port 162 must be open for User Datagram Protocol (UDP) traffic on all potential firewalls between Venafi Log server to the SNMP console. You can configure the firewalls accordingly.
- If the SNMP host only supports IPv4 traffic, you can configure the channel for SNMP v1. For more information, see "SMTP outbound server configuration" on page 451.

- Be sure the IIS bindings for Trust Protection Platform match the host SNMP settings. For example, if the SNMP host uses the IPv6 protocol, you can add a binding in IIS.
- If the SNMP host supports IPv4, IPv6, or a dual stack implementation, you can configure the channel for SNMP v2c or SNMP v3. Be sure the IIS bindings for Trust Protection Platform match the host settings.
- If there are multiple SNMP hosts that use more than one SNMP version, you must create a SNMP channel for each version.
- Ensure proper channel configuration. The SNMP driver does not buffer traps that are undeliverable because of a misconfiguration or a server failure.
- For each SNMP channel object, you must generate and distribute the *venafi.mib file* to the SNMP management console. Whenever events change, for example you upgrade to a new version of Trust Protection Platform, you can regenerate and redistribute the .mib file. For more information, see "Customizing the Management Information Base" on page 493.

SNMP Channel object configuration

The Simple Network Management Protocol (SNMP) Channel object stores the information the SNMP driver needs to send traps to an SNMP management system. You must have the Read and Write permission to the Log Application objects in the Logging Tree.

The following table provides a description of configuration settings for the SNMP Channel object.

Field	SNMP Version[1]	Description
Host	all	Hostname or IP address of the SNMP management system that receives Trust Protection Platform event notifications as trap messages. If a hostname is specified, only the first resolved address associated with that name is used.
SNMP Version	all	The setting that matches the host SNMP version. This setting works in conjunction with the matching section of additional configuration settings on the page. ■ *SNMP v1*: Uses a single trap OID for all events. Supports IPv4 connections between Trust Protection Platform and the host. ■ *SNMP v2c*: Generates traps with unique OIDs for each event. Uses its own MIB file with Trust Protection Platform event mappings to OIDs. The OIDs include the Trust Protection Platform event fields and descriptions so administrators can look for specific traps in their monitoring systems. Supports IPv4, IPv6, or IPv4/IPv6 dual stack configurations. ■ *SNMP v3*: Generates traps with a unique OIDs for each event. In addition to the same features as SNMP v2c, SNMP v3 provides encryption. Supports IPv4, IPv6, or IPv4/IPv6 dual stack configurations. **NOTE** If you change the MIB file, be sure to use the GenerateMIB utility to update the file. For more information, see "Customizing the Management Information Base" on page 493.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

Field	SNMP Version[1]	Description
Trap OID	v1	(Optional) The Object ID to associate with all traps that originate in Trust Protection Platform. The default is *1.3.6.1.4.1.28783.1.1*.The default OID was registered by Venafi for private use by enterprises. For more information, see http://www.oid-info.com/get/1.3.6.1.4.1.28783.
Message	v1	(Optional) The text that appears in the message body for all traps sent from this SNMP Channel object. Because SNMP specifications require that an SNMP packet can be no larger than 500 bytes, the message body is limited to 300 bytes. The SNMP driver simply truncates anything over 300 bytes. The SNMP notification message can be dynamically derived from the event using the Trust Protection Platform macro language.
Community	v1, v2c	Community string to access the SNMP management system.
Username	v3	Defines the username used to authenticate to the SNMP console when sending a trap.
Engine ID	v3	Defines the EngineID, used in the SNMP v3 protocol, to uniquely identify the Logging Server as an SNMP Engine.
Authentication	v3	Enables or disables SNMP v3 authentication.
Protocol	v3	Works in conjunction with **Authentication**. Defines the hashing algorithm, *SHA1* or *MD5*, used when SNMP v3 authentication is enabled. *SHA1* is the default hashing algorithm.
Passphrase	v3	Works in conjunction with **Authentication**. The password credential object used to authenticate to the SNMP console.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

Field	SNMP Version[1]	Description
Privacy	v3	Works in conjunction with **Authentication**. Enables or disables SNMP v3 privacy encryption.
Protocol	v3	Works in conjunction with **Privacy**. Defines the encryption protocol *AES* or *DES*. *AES* is the default.
Passphrase	v3	Works in conjunction with **Privacy**. The password credential required to authenticate to the SNMP console.

Customizing the Management Information Base

For each Simple Network Management Protocol (SNMP) channel object, you must generate and distribute the *venafi.mib* file to the SNMP management console. If you change event definitions, or if you upgrade to a new version of Trust Protection Platform, you can should and redistribute the .mib file.

To generate the file, you run the GenerateMIB utility. GenerateMIB maps events to specific Object Identifiers (OID)s in the .mib file. The OIDs include the Trust Protection Platform event fields and descriptive event text so administrators can look for specific traps in their monitoring systems.

To generate the Venafi Trust Protection Platform MIB file

1. Open Venafi Configuration Console (VCC) or the Venafi Tools MMC Snap-in.

   NOTE You must have `Read, Write` permission to the event definitions.

2. Open the **Tools** > **Logging** > **Event Definitions** node and make the desired changes.

   Now that the event definitions have changes, you need to actually generate the .mib file.

3. On the Venafi Platform server, open a command prompt.

[1]Depending on the SNMP version you select, the rest of the fields on the form change. This column shows which settings apply to which SNMP versions.

4. Browse to the `[drive]:\Program Files\Venafi\Platform` directory.
5. Run the `GenerateMIB.exe` utility:

   ```
   Generatemib.exe [-n:<mibname>] [-m:<modulename>] [-o:<outfile>] -c [-?|-h]
   ```

   Example:

   ```
   Generatemib.exe -n:VENAFI-MIB -m:MyCustomName -o:VENAFI-MIB.txt -c
   ```

   The `-m` switch is optional and allows you to provide a custom module name that will be displayed in your SNMP management system.

   The `-c` switch should always be used and ensures the data is refreshed from the configuration.

   This program creates the `venafi.mib` file in the current directory.

   An example of a customized MIB entry is the following:

   ```
   customizedNoCATemplate NOTIFICATION-TYPE
   OBJECTS { eventComponent, eventSeverity, eventClientIpAddressType, eventClientIpAddress,
   publicKeyFingerprint-11, certificateFolder, translatedEvent }
   STATUS current
   DESCRIPTION "Customized - No CA Template"
   ::= {director 3276817}
   ```

6. Distribute the MIB file to the SNMP management console.
7. Each time you change event definitions, re-run the `GenerateMIB` utility and redistribute the resulting `venafi.mib` file.

About syslog channels

A syslog channel allows the Venafi Log server to send log messages to any log aggregation or analyzer solution that supports the syslog protocol. Instead of a local timezone, log messages contain the GMT/UTC timestamp from the Trust Protection Platform server.

Trust Protection Platform version 19.3 introduced two new message formats–Common Event Format (CEF) and JSON–and can now support encrypted (TLS) connections to remote syslog servers. The legacy BSD format remains available.

All Venafi Log server messages include a severity code, which aligns with standard syslog severity codes. For example, 3 represents an error, 4 represents a warning, etc. Also, channel configuration settings lets administrators specify syslog facility codes.

About the CEF format

CEF, or Common Event Format, is a standardized logging format used by many network devices and applications. CEF logs contain information like the source and destination of an event, its severity, its event ID, and the message.

If the Syslog server records messages in the CEF format, the timestamps are recorded as local server time. If you are working with servers in multiple timezones, you need to be aware that per the CEF specification, dates are recorded in UTF format.

About the JSON format

If the Syslog server records messages in the JSON format, the timestamps are local time. When you select JSON as the message body format, it uses the following pattern:

```
{
  "time_stamp":"<Event.ClientTime>",
  "name":"<Event Description from Log Schema>",
  "event_id":"<Event.ID>",
  "severity":"<Event.Severity>",
  "dvc_ip":"<Event.SourceIP>",
  "object":"<Event.Component>",
  "object_id":"<Event.ComponentId>",
  "object_subsystem":"<Event.ComponentSubsystem>",
  "text1":{
    "name":<Text1 Title from Log Schema>,
    "value":<Event.Text1>
  },
  "text2":{
    "name":<Text2 Title from Log Schema>,
    "value":<Event.Text2>
  },
  "value1":{
    "name":<Value1 Title from Log Schema>,
    "value":<Event.Value1>
  },
  "value2":{
    "name":<Value2 Title from Log Schema>,
    "value":<Event.Value2>
  },
  "grouping":{
```

```
    "name":"<Grouping Title from Log Schema>",
    "value":"<Event.Grouping>"
  },
  "data":{
    "name":"<Data Title from Log Schema>",
    "value":"<Event.Data>"
  }
}
```

About the BSD format

The legacy Berkeley Software Distribution (BSD) format continues to be supported. If the Syslog server records messages in the BSD format, the timestamps are GMT/UTC time. For more information about BSD, see https://tools.ietf.org/html/rfc3164.

About TLS

Syslog channel driver can establish secure (encrypted) connection over TLS to the remote destination.

Syslog channel prerequisites

To enable the Venafi Log server to send log messages to a syslog server, ensure that you meet the following prerequisites:

- You must know the IP address or hostname of your syslog server.
- Update your firewall rules to match the port and protocol that you plan to use.

  Typically, opening firewall rules for UDP port 514 won't allow TCP traffic on that port. If you use TLS, you should select the standard port of 6514 (per RFC 5425: https://tools.ietf.org/html/rfc5425.
- Configure your syslog server to parse the message format you choose (CEF or JSON).

Syslog servers accept any message. However, if you don't configure them to parse the specific format, messages won't be captured in a way that can be consumed by Security Information and Event Management (SIEM) solutions.

To configure a syslog channel object

The Syslog Channel object stores the information that the Venafi Log server needs in order to send log messages to a syslog server.

IMPORTANT Syslog channel drivers can't recognize changes you make to either the **Allowed Outbound SSL/TLS Versions** settings or **Certificate Versions** settings. Therefore, following any changes to those settings, please restart the Venafi Log Server Windows service. For details, see "Manually stopping and starting the log server service" on page 432 in the *Log Server Administration Guide*.

To configure a syslog channel

1. In Venafi Configuration Console (VCC), navigate to **Tools** > **Logging** > **Channels**.
2. Right-click **Channels**, and then point to **Add** > **Syslog**.

   Refer to the following table while configuring your syslog channel object:

Field	Description
Host	IP address or hostname of the syslog server where you want the Venafi Log server to send log messages. The target host might look similar to one of the following examples: ◦ syslog_server.example.com ◦ 192.0.2.1 ◦ fd9d:1645:7e28:f043:6920:b203:cbe3:54ef
Format	Specify the format you want to use for your syslog messages by selecting one of the following: ◦ **BSD (Legacy)** For more information, see "About the BSD format" on page 496. ◦ **Common Event Format** (CEF) For more information, see "About the CEF format" on page 495. ◦ **JSON** For more information, see "About the JSON format" on page 495.
Facility	Facility code for the syslog channel. This option is available only if you use the BSD format. A facility code is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently. By default, the Syslog channel uses facility 16, or Local0, which is the first unassigned facility value in the list. For more information on syslog facility values, consult RFC 3164 (https://tools.ietf.org/html/rfc3164).
Protocol	Select either TCP or UDP (the default). The *user datagram protocol* (UDP) has been the most common transport layer protocol for network logging with the server listening on port 514. As UDP lacks congestion control mechanisms, TCP must be used for situations where *transport layer security* (TLS) is required.
Port	Specify the port of your syslog server.

Field	Description
	By default, the Syslog channel uses UDP port 514. To change the port number, specify it here. For example, if you want to use UDP port 1022, select the UDP protocol and type 1022 in the Target Port field.
Use TLS (Conditional)	(Conditional) If you want to establish an encrypted TLS connection to a remote syslog server, you must select TCP as the protocol and set Enable TLS to **Yes**.
Certificate	(Optional)(Conditional) If you enabled TLS, you can select a certificate credential in cases where the remote syslog server requires authentication using a specific client certificate.

3. When you're finished, click **OK**.

7

Working with notification rules

Notification rules send logging information for specific events to the defined channels.

IMPORTANT Your default log channel receives all events. Notification rules are used to send the logs of specific events to a channel other than your default channel. Do *not* send notifications to your default logging channel because this results in duplicate logged events.

This chapter contains the following topics:

Notification rule editor operators 504

Notification rule variables and supported operators 505

Login failure notification 507

Successful login from unknown IP address notification 507

Showing the correct IP address when using a load balancer to show the correct IP address 508

Working with Venafi Platform 509

Using the TppConfiguration command line tool 511

Using TppTool from the command line and script files 519

Using the TppPKIs command line tool 524

Creating notification rules

Notification rules connect events with channels so that the event's logging information can be passed along to the specified channel.

Trust Protection Platform provides several default notification rules you can edit or use to create new notification rule objects.

Notification rules can be seen as a type of filtering tool. They contain filtering criteria that either match or don't match system events. For each system event, the log server checks each notification rule to see if its rules match the event. If it matches, the log is passed to the channel (or channels) configured for the notification rule. If the event doesn't match the notification rule, the system takes no additional action.

You use notification rules to tell the system which events are important to you, and what logging action to take when one of those events occurs. These logging actions are defined in channels.

Notification rules answer the question "What events are important?" Channels answer the question "What should happen when an important event happens?"

For example, if you want to email important events to your mailbox, you must select an SMTP channel that is configured to relay events to your email address. Similarly, if you want to log specific events to a MS SQL database, you must select a MS SQL channel that is configured to write the events to the correct database and table. You can define multiple channels for any given notification rule.

To create a notification rule:

1. In Venafi Configuration Console (VCC) or the Tools MMC Snap-in, open **Tools** > **Logging** > **Notification Rules** .

   > **NOTE** You must have `Create, Write` permission to the Notification Rules folder.

2. In the Actions panel, click **Create new notification**.

   To use an existing rule as a template, you can also choose a pre-configured rule from the **Built-In** list, then click the **Duplicate** action.

3. In the **Add Notification** dialog, specify a name for the notification rule , and then click **Add**.

4. Complete the notification rule configuration, and then click **Apply**.

The following table outlines the configuration settings for notification rules.

Field	Description
Description	A short explanation of the purpose of the rule. This will be displayed at the bottom of the Actions Panel in the Description section.
Target Channels	Channel objects the Venafi Log server uses to provide event responses or log the events. Click the Search box to load a list of channels. You can select multiple channels for any given notification rule.
Notification Disabled	Disables the current Notification Rule object.
Edit the Rule	Opens the Rule Editor. The Rule Editor is described in the following section.

Working with the Rule Editor

The Rule Editor is where you compose and test your notification rules. It has the following sections:

- **Rule Text.** This is the editor where you create your rules. While the rule is valid, you see a green check at the top of the section. When the rule is not valid, you see a red X. As you are typing, the upper-right corner of the section gives feedback on how the rule is interpreted or where it thinks there may be errors.

  Press `Ctrl + H` to see the auto-complete help window. Depending on context, the auto-complete will show what options or operators are valid. The operators are described in the table in the next section.

  You can't save the rule unless it is evaluated as being a valid rule.

- **Sample data.** Below the rule text is a series of fields where you can enter sample data. This helps you see the notification results, and helps you target your rule for specific conditions.

- **Rule Analysis.** For valid rules, it shows the order the logic is processed. This can be really helpful for complex notification rules, so you can ensure the rule text is evaluated the way you expect.

- **Processing Result.** Shows how the rule would process, based on the rule text and the sample data. If the rule and sample data combination would generate a notification, you see a green check. If the rule and sample data combination would not generate a notification, you see a red stop sign. This

section then shows why it returned that result, helping you fine tune your notification rule.

- **Event Browser.** Shows all the defined system events. Click once on an event to see the sample data for that event. Double-click on an event to add that event's ID to the Rule Text.

  Use the Filter box to find specific events. The filter matches both the event category and the event name.

Notification rule editor operators

The notification rule language is human readable and writable. It supports bracketing, boolean operators, short-circuit decisions, and allows complex decisions to be expressed.

The following table shows all the operators that are supported. To see which variables can use which operators, see the next section.

Operator	Syntax[1]	Description
== (Equals)	`a == b`	Compares if `a` is equal to value `b`. Returns `true` if they are equal, otherwise returns `false`.
!= (Not Equals)	`a != b`	Compares if `a` is not equal to value `b`. Returns `true` if they are not equal, otherwise returns `false`.
IN	`a in [0010, 0020,0030]`	Checks if value `a` is present in the specified `[group]`. Returns `true` if it is, otherwise returns `false`. The group is a comma separated list inside square brackets.
IS	`a IS EMPTY`	Argument must be one of: ■ **Empty** - Null or empty string ■ **DN** - Value is DN ■ **Number** - Value is a number ■ **Letters** - Value is only letters ■ **Whitespace** - Value is only whitespace

[1] String arguments should be entered with quotation marks.

Operator	Syntax[1]	Description
MATCHES [2]	`MATCHES "\\\\VED\\\\Policy\\\\.*"`	Argument is a regular expression and variable must have a match to be TRUE.
LIKE	`LIKE "rest"` or `LIKE "198.51.100.14/24"`	For strings, acts as a "contains." For IP address: Argument is CIDR, and Source IP must be part of CIDR range.
<	`a < b`	Checks if value `a` is numerically less than value `b`. Returns `true` if it is, otherwise returns `false`.
>	`a > b`	Checks if value `a` is numerically greater than value `b`. Returns `true` if it is, otherwise returns `false`.
<=	`a <= b`	Checks if value `a` is numerically less than or equal to value `b`. Returns `true` if it is, otherwise returns `false`.
>=	`a >= b`	Checks if value `a` is numerically greater than or equal to value `b`. Returns `true` if it is, otherwise returns `false`.
&&	`a && b`	Logical AND. Returns `true` if both `a` and `b` are `true`. Otherwise, returns `false`.
||	`a || b`	Logical OR. Returns `true` if either `a` or `b` is `true`. Otherwise, returns `false`.
!	`!a`	Logical NOT. Inverts the value of `a`. Returns `true` if `a` is `false`, and `false` if `a` is `true`.

Notification rule variables and supported operators

The following table shows the supported variables, and what operations are allowed for each variable.

[1] String arguments should be entered with quotation marks.

[2] Regular expressions are only supported using the `MATCHES` operator, and use .NET regular expression syntax. See "Using regular expressions in a notification rule" on the next page.

Variable	Example	Rules					
		== !=	< <= > >=	LIKE	MATCHES	IS	IN
Component	`\VED\Policy\Abc`	✓		✓	✓	✓	✓
Data[1]	`Some Text`			✓	✓	✓	✓
EventID	`0x001f0003`	✓	✓				
Grouping	`154`	✓	✓				✓
Severity	`Info`	✓	✓				✓
SourceIP[2]	`192.168.3.4/24`	✓		✓			✓
Text1	`Some Text`	✓		✓	✓	✓	✓
Text2	`Other text`	✓		✓	✓	✓	✓
Value1	`123`	✓	✓				✓
Value2	`456`	✓	✓				✓

Using regular expressions in a notification rule

Regular expressions allow you to search for patterns of data such as email addresses or IP addresses. In Venafi Trust Protection Platform, regular expressions are used in Notification Rules to search for patterns of data using the `MATCHES` operator. In Venafi Platform, RegEx follows the .NET Framework syntax.

For example, the following regular expression searches for an Internet email address:

```
\b[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}\b
```

If the event data in the designated field matches the pattern specified in the regular expression–i.e., an Internet email address–the event triggers the Notification Rule and a notification is sent via the designated target channels.

For more information on regular expressions, see:

.NET Framework Regular Expressions (http://msdn.microsoft.com/en-us/library/hs600312.aspx)

and

Regular Expression Language Elements (http://msdn.microsoft.com/en-us/library/az24scfc.aspx).

---

[1]Data is assumed to be encoded UTF-8 text and converted to UTF-8 before operators are applied.
[2]SourceIP supports both IPv4 and IPv6 addresses and CIDR notation.

Configuring expiration event intervals

You can define the intervals at which Trust Protection Platform generates expiration events for certificates, symmetric keys, and SSH keys at the object level in individual Certificate, SSH key, or Symmetric Key objects; or you can manage the expiration event intervals via policy.

The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in notification and channel objects. By default, Trust Protection Platform provides default notification rules for expiration events. You can see these rules in Venafi Configuration Console (VCC), or in the Tools MMC Snap-in collection.

Configuring your system for login notifications

Venafi Platform ships with two default email notifications for login security. These notifications help secure your environment by alerting users to successful login attempts from unknown IP addresses, as well as all unsuccessful login attempts. These notifications are enabled by default.

Each of these notifications is described below, followed by important configuration information if you are using a load balancer.

Login failure notification

It is important that users be alerted any time an attempt to log in fails in case somebody is trying to break into their account. This notification will trigger anytime a user attempts to log in to Venafi Platform but the login attempt fails. This may be due to an incorrect password, or another authentication issue.

This notification goes to the user whose login was used in the login attempt, and includes the IP address of the user attempting to log in.

The notification rule in VCC is called **Login Failure**, and is in the Built-In folder.

The target channel is called **Email to Owner - Login Failure**.

The subject of the email is "Account Login Failure".

Successful login from unknown IP address notification

Sometimes you want users to be notified anytime a login happens from an unknown IP address. This notification triggers anytime a user successfully logs in to Venafi Platform from an unknown location (as determined by IP address). This notification goes to the user who successfully logged in, and includes

information about the login, including the IP address of the user who successfully logged in. This notification is important because it helps users monitor logins from remote locations. If a user doesn't recognize a location, their account information may be compromised.

IP history is stored with each user's preferences, so if users clear their preferences (**User menu** > **My Account** > **Reset Settings & Preferences**), their location history will also be reset.

The notification rule in VCC is called **Login Successful from Unknown Source**, and is in the Built-in folder.

The target channel is called **Email to Owner - Login Successful**.

The subject of the email is "Account Login from New IP Address".

Showing the correct IP address when using a load balancer to show the correct IP address

If you are using a load balancer, you need to configure the load balancer to log the `X-Forwarded-For` header. If the load balancer is not configured correctly, these notification will show the IP address of the load balancer. This is especially important for the successful login notification, because without the `X-Forwarded-For` header on the load balancer, the notification is essentially meaningless, since *all requests* will appear to be coming from the load balancer.

Logging the `X-Forwarded-For` header provides better security logs for web activity that comes through a load balancer, and will help you troubleshoot your load balancer. (If you are not sure if your load balancer is properly configured to send the `X-Forwarded-For` header, you can check your IIS logs on your Venafi server.)

This is done in two steps: 1. Configure your load balancer to pass the client IP address in the `X-Forwarded-For` header; and 2. Configure your Venafi server IIS settings to log the `X-Forwarded-For` header.

To configure your load balancer

- Check your load balancer vendor documentation for specific steps on configuring the `X-Forwarded-For` header.

You can read reference information about the `X-Forwarded-For` header on MDN Web Docs.

To configure your Venafi server's IIS settings to log the `X-Forwarded-For` header

1. Connect to your remote Venafi server, and open Internet Information Services (IIS) Manager.
2. In the **Connections** panel, expand **Sites**, and click **Venafi**.
3. In the IIS group, double-click **Logging**.
4. Under the Log File section, click the **Select Fields** button next to the Format: W3C dropdown.
5. Click **Add Field...**
6. Set the following values:

Field	Value
Field Name	X-FORWARDED-FOR
Source Type	Request Header
Source	X-FORWARDED-FOR

7. Click **OK** to close the Edit Custom Field window.
8. Click **OK** to close the W3C Logging Fields window.
9. Restart IIS to ensure settings take effect.

When IIS restarts, the correct IP addresses will appear in the login notification email messages for all users in your organization, and will be logged on the Venafi server.

Working with Venafi Platform

The Platform product is the underlying architecture upon which Venafi Trust Protection Platform products are built. The Venafi Platform product allows you to configure options and settings that are independent of a specific product like TLS Protect or SSH Protect.

Venafi Platform can only be seen by users who are master administrators, or who have `View` and `Read` permissions to the `\VED\Engines` object.

You do not need an active Venafi license to access Platform.

Access Platform from the context switcher, next to the user icon on the menu.

Platform has the following features:

- **System Status (dashboard).** This dashboard shows you license counts and information about engines connected to the Trust Protection Platform database.

  For more information, see "Working with the System Status (dashboard)" on page 629.

- You can use TppTool to perform Venafi Platform actions through the command line or script files. See" Using TppTool from the command line and script files" on page 519.

- **Venafi Servers.** This menu takes you to the classic policy tree, and shows you the **Platforms tree,** where you can see all the engines connected to the database, and you can configure settings related to the servers, individually or collectively.

  For more information, see Platform Objects.

- **Policy Tree.** This menu takes you to the classic policy tree view, and shows you the **Policy tree**. The Policy tree provides a hierarchical view of your encryption deployment model. Policy items (for example, devices, applications, CA templates, certificates, credentials, and so on) display in context of other system objects so you can intuitively design your object hierarchy and policy inheritance paths.

  For more information on managing policies, see "Using policies to manage encryption assets" on page 859.

- **Encryption.** This menu takes you to the classic policy tree, and shows you the **Encryption tree** which contains your system's Encryption drivers. Encryption drivers provide access to the keys used to secure your system's encryption assets—that is, certificates, private keys, SSH keys, Credential objects, administrator usernames and passwords, and all other information stored in the Secret Store database.

  For more information about the Encryption tree, see "Managing system encryption keys" on page 545.

- **Notifications.** This menu takes you to the classic policy tree, and shows you the **Notification Rules node** of the **Logging tree** which provides a comprehensive view of the Trust Protection Platform notification system and is the control center for all system logging and notification activities.

  For more information, see "Understanding system logging and notifications" on page 983.

- **API > Default Settings.** The Default Settings allows you to configure the default configurations for API access, including allowed authentication methods, token refresh settings, and session caching. These settings can also be found in the Venafi Configuration Console.

For more information see "API default settings for remote access configuration" on page 763.

- **API > Integrations.** The Application Integrations menu link takes you to the **API Integrations** list. Here a master administrator can create app integrations that manage scopes and restrictions of identities needed for accessing specific subsets of API methods. Fundamentally, this feature is about limiting an external application's ability to call some methods within APIs while restricting others via the identities used to access the API.

  For more information, see "About API integrations" on page 750.

- **Clients > Client Group Settings**. The Client Group Settings menu takes you to the groups list where you can better manage SSH key and certificate management work on machines in your environment.

  For more information, see Working with Client Group Settings.

- **Clients > Work Settings.** The Work Settings allows you to configure Discovery work, and set placement rules either through an agent on the target device, or through an agentless discovery.

  For more information, see Creating and assigning Work.

- **Clients > Registered Clients.** The Registered Clients list shows you a list of all discovered client devices, with a variety of details about the client including the operating system, credential, and when the device last connected.

  For more information, see Working with Group and Server Agent details.

- **Clients > Agent Registration Settings.** The Agent Registration Settings lets you configure Server Agent settings for each agent that connect to Trust Protection Platform.

  For more information, see Configuring Server Agent registration.

- **Logs.** The Logs menu link takes you to the Classic Policy Tree and shows you **the Default SQL Channel node**, which enables Venafi Platform to record events to a Microsoft SQL Server database (either you primary Trust Protection Platform database, or a separate database as needed).

  For more information about logging and notifications, see "SQL Server channel" on page 443.

Using the TppConfiguration command line tool

Venafi Platform includes a command-line utility that allows system admins to perform installation and configuration actions through the command line or through script files. It provides administrators with greater flexibility and automation capabilities when managing the platform, especially when dealing with

multiple environments or large-scale deployments.

The utility is called TppConfiguration.exe and exists in the installation directory, in the following location (assuming you used the default installation directory):

```
C:\Program Files\Venafi\Platform\TppConfiguration.exe
```

This utility requires you to use an elevated command prompt.

How to open an elevated command prompt

1. From the Start menu, search for `CMD`.
2. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Using the TppConfiguration command, administrators can:

- Script the installation or upgrade of Venafi Platform on servers.
- Update the database connection information for a Venafi Platform server.
- Enable access to the MMC snapins for the current Windows user.
- Update the company name or installation type of a server.
- Uninstall Venafi Platform.
- Update the HSM pin.

When using the command line utility to install, configure, upgrade, or uninstall Trust Protection Platform, there are a number of allowed switches. This utility requires you to use an elevated command prompt.

The command line argument is:

```
TppConfiguration.exe -<switch>=<value> -<switch2>=<value>
```

Some switches require master admin authentication. They are noted in the table below. When you use a switch that requires master admin authentication, you can either:

- Provide the `-username` and `-password` inline in the command. (Required if you are scripting the command.)
- Wait until prompted by the application to enter the master admin credentials.

TPPConfiguration syntax

- The command line tool uses a flexible syntax. Simply run the `TppConfiguration` program with parameters to perform specific tasks.

  For example, `TppConfiguration -errorcodes` will output a list of return codes and a description of the error. Neither commands or parameters are case sensitive, meaning `tppconfiguration -errorcodes` and `TppConfiguration -errorcodes` and `TPPCONFIGURATION -ERRORCODES` are all interpreted the same.

- To perform specific tasks, type a parameter directly after typing the `TppConfiguration` command. For instance, `Tpponfiguration -enablemmc`.

- When running the program with no parameters, you will see the inline help. There, you will see that some characters in parameter names are bolded and some are not. The bolded characters are a short-cut syntax that makes it quicker and easier to type commands. For example, the `add` parameter is displayed in the inline help as `-**a**dd`. The bolded part, in this case `-a`, is the short cut.

  This short-cut syntax can make it quicker and easier to type commands; however, to ensure compatibility with future versions of TPPConfiguration, you should use full parameter names when scripting.

  > **TIP** The hyphen (`-`) is technically optional, but is recommended for forwards compatibility.

- Command options are additional modifiers that provide further instructions or information to the TPPConfiguration command being executed. For example, `-username=<master-admin-user>` is used to indicate the username of the master administrator account needed to perform the action. The tool accepts the following operators: `=`, `:`, and ` ` (space). Thus the following examples are all treated the same: `-username=venafi`, `-username:venafi`, and `-username venafi`

Combining these principles, the following commands are all interpreted the same:

```
TppConfiguration -enablemmc -username=george.washington -password=Passw0rd!11
```

```
tppconfiguration enablemmc username george.washington -password Passw0rd!11
```

```
TppConfiguration.exe -ENABLEMMC -username:george.washington pa:Passw0rd!11
```

```
tppconfiguration ena us:george.washington pa Passw0rd!11
```

Configuration switches for TppConfiguration.exe command line tool

Click a column header to sort by that column.

Parameter	Type	Auth[1]	Description
`-errorcodes`	Common Options	No	Show all error codes that may be returned.
`-password:<pw>`	Common Options	Yes	Password to decrypt the answer file.
`-username=<name>`	Common Options	No	User name of local Venafi Platform admin account.
`-keyexport=<pem>`	Configuraiton	Yes	Exports the default software key. (Requires `-password`)
`-dboconfig=<cfg>`	Configuration	No	Allows changing the SQL database owner account connection information from the command line. You can use this, for example, for automated updating of the SQL database owner account password. For details on the connection string and its proper syntax, see "Obtaining the SQL database connection string" on page 59.
`-keyimport=<pem>`	Configuration	Yes	Imports the default software key. (Requires `-password`)

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth[1]	Description
`-sqlconfig:<cfg>`	Configuration	No	Allows changing the SQL operational account connection information from the command line. You can use this, for example, for automated updating of the SQL operational account password. For details on the connection string and its proper syntax, see "Obtaining the SQL database connection string" on page 59.
`-add`	Installation	No	Runs the installer in the mode that adds this Venafi server to an existing Venafi server cluster (servers that share a single database).
`-install=<xml> -password=<pw>`	Installation	No	Runs the installer (fresh install if DB is empty; upgrade if DB is not empty) with the configuration options specified in the answer file, and supplies the password to decrypt the answer file. For example, if the answer file is located at `c:\answerfile.xml` and the decryption password for the file is `Example"Password`, this switch would be: `-install:C:\answerfile.xml -password:Example\"Password`

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth[1]	Description
			NOTE The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it as `pas\"sw\\ord`.
`-log=<file>`	Installation	No	Allows you to override the default location of the log file where the results of the configuration process are stored. If you want to save the log file at `C:\Temp\VenafiLog.txt`, the switch would be: `-log:C:\Temp\VenafiLog.txt`
`-uninstall`	Installation	No	Uninstalls Trust Protection Platform from the Venafi server by doing the following: ■ Removes Venafi registry values, and backs up settings to a registry file stored in the same folder as the log file. ■ Removes the Venafi website from IIS.

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth[1]	Description
			This switch is used by Windows when you use Program Features to uninstall Trust Protection Platform. **NOTE** This does not remove the files or Windows Services installed by the .msi. It only removes the websites and registry entries.
`-company=<name>`	Miscellaneous	Yes	Sets the company name for the system.
`-decrypt=<xml>`	Miscellaneous	Yes	Decrypts the specified XML file. (Requires `-password`)
`-deployment=<t>`	Miscellaneous	Yes	Sets the deployment type for the system. Allowed values for `<t>` are: ■ `D` - Development ■ `T` - Test ■ `S` - Staging (pre-production) ■ `U` - User Acceptance Test (UAT) ■ `P` - Production
`-encrypt=<xml>`	Miscellaneous	Yes	Encrypts the specified XML file. (Requires `-password`)
`-help`	Miscellaneous	No	Shows a help file in the command line window, describing these features and settings.

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth[1]	Description
`-dbgrant=<user>`	Recovery	Yes	Provides the necessary grants to the Venafi database for the specified user to be an operational database service accounts. This is helpful when using Windows Authentication and users need to launch WebAdmin or Venafi Support Tool.
`-driverpwd=<new-pw>`	Recovery	Yes	Requests to change the service account password of an identity connector. `<new-pw>` is the new password. Uses `-name`, `-username`, and `-password` and will prompt if any are omitted.
`-enablemmc`	Recovery	Yes	Adds or replaces MMC access grant for the current user. Use `-username:` and `-password:` to provide Trust Protection Platform user credentials on the command line. Otherwise, you will be prompted for credentials.
`-hsmpin=<pin>`	Recovery	No	Allows setting the HSM PIN in an HSM-only environment. This is necessary if the HSM pin has been changed, and needs to be updated in Trust Protection Platform. Note: When used without the <pin> argument, you will be prompted for the pin.

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth[1]	Description
`-name=<cn>`	Recovery	Yes	The common name of an identity connector object.
`-distrust=<dll>`	Trust	No	Allows you to remove a DLL from being a trusted resource.
`-trust=<dll>`	Trust	No	The path to a custom DLL, allowing it to be added as a trusted resource. For custom development modules, this feature adds the signature of the custom module as trusted resource so the custom features can be added to Trust Protection Platform.

You can combine the switches as needed. For example, here is a command line argument that installs the software on this Venafi Trust Protection Platform server, while connecting to an existing database using a configuration file, and overwriting the default log file location:

```
TppConfiguration.exe -in=C:\answerfile.xml -add -pa=Washington -
l=C:\Temp\VenafiLog.txt
```

Using TppTool from the command line and script files

TppTool is a command-line utility that lets system administrators (and in some cases schema administrators) perform Venafi Platform actions through the command line or script files. It provides administrators with greater flexibility and automation capabilities when managing the platform, especially when dealing with multiple environments or large-scale deployments.

Using the TppTool command, administrators can:

[1]Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

- Export and import various components of the Venafi Platform configuration, such as objects, attributes, policies, and permissions. This makes it easier to copy settings between environments, back up and restore specific configurations, and generate reports on the current system setup. Please note that TppTool is available in addition to Schematool.exe, which is still available for backward compatibility.
- Manage the recycle bin, including restoring accidentally deleted objects, permanently deleting all objects or specific items from the recycle bin, and scheduling automatic purge and deletion tasks. Please note that these tasks can also be performed by using Venafi Configuration Console. See "Venafi Recycle Bin" on page 138. TppTool replaces the TPPRecycleBin.exe command.
- Interact with and manage the Daily Tasks engine, which controls settings across the platform and determines when they will run. TppTool replaces the TPPDailyTasks.exe command.
- Users with the Schema Administrator role can export and import Venafi Platform objects using TppTool, as long as they have permissions to the objects.

TppTool syntax

- The TppTool program is located at: `[InstallDir]\Platform\TppTool.exe`.
- To perform specific tasks, type a parameter directly after typing the `TppTool` command. For instance, `TppTool -version`. Please note that commands and parameters are **not** case-sensitive, meaning `TppTool -version` and `TPPTOOL -VERSION` are interpreted the same.
- When running the program with no parameters, you will see the inline help. There, you will see that some characters in parameter names are bolded and some are not. The bolded characters are a short-cut syntax that makes it quicker and easier to type commands. For example, the `version` parameter is displayed in the inline help as `-**v**ersion`. The bolded part, in this case `-v`, is the short cut.

  This short-cut syntax can make it quicker and easier to type commands; however, to ensure compatibility with future versions of TppTool, you should use full parameter names when scripting.

  > **TIP** The hyphen (`-`) is technically optional, but is recommended for forwards compatibility.

- Command options are additional modifiers that provide further instructions or information to the TppTool command being executed. For example, `-cryptpw=<password>` is used to provide the password for encrypting and decrypting XML files, and `-username=<name>` is used to provide a valid username that is allowed to complete the operation. The tool accepts the following operators: `=`, `:`, and ` ` (space). Thus the following examples are all treated the same: `-u=venafi`, `-u:venafi`, and `-u venafi`

Combining these principles, the following commands are all interpreted the same:

```
TppTool -startrotation -platform=Venafi1 -connector=hsm1
```

```
TPPTOOL.exe startrotation platform Venafi1 connector hsm1
```

```
tpptool startrotation -platform:Venafi1 -conn=hsm1
```

TppTool parameters and options

Click a header to sort by that column.

Parameter	Type	Description
`-password=<pass>`	Common options	Provide a password (prompted if omitted). **NOTE** The quotation mark `"` and backslash `\` characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is `pas"sw\ord`, you would enter it as `pas\"sw\\ord`.
`-username=<name>`	Common options	Provide a username.
`-daily`	Daily tasks	Trigger Daily Tasks action.
`-notify`	Daily tasks	If specified, any applicable notifications will be resent when triggering Daily Tasks action.
`-cryptpw=<password>`	Import & export options	Provide the password for encrypting and decrypting XML files. Export will be in

Parameter	Type	Description
		cleartext if not provided.
`-connector=<hsm>`	Key Rotation	If specified, the connector the new key should be stored on. If omitted, the connector of the existing system protection key will be used.
`-disablesw`	Key Rotation	When rotating from software to hardware, disable the software key after rotation is complete.
`-keyname=<name>`	Key Rotation	The name of the new key. The key must not exist. It will be created on the specified connector during rotation.
`-platform=<tpp-server>`	Key Rotation	The name of the Venafi Platform server that should perform the key rotation. If omitted, the first available server is used.
`-startrotation`	Key Rotation	Create a request to rotate the system protection key. Requires `-keyname`. You can optionally specify the `-connector` and `-platform`.
`-stoprotation`	Key Rotation	Abort any outstanding key rotation requests.
`-column`	Recycle Bin options	For `-show`: Display contents in columns.
`-guid=<bin-guid>`	Recycle Bin options	For `-purge`/`-restore`:

Parameter	Type	Description
		The GUID of the item to purge or restore.
`-bin`	Recycle Bin tasks	Perform the recycle bin action.
`-contents`	Recycle Bin tasks	Display the contents of the recycle bin.
`-empty`	Recycle Bin tasks	Empty the recycle bin.
`-purge`	Recycle Bin tasks	Purge a deleted item from the recycle bin.
`-restore`	Recycle Bin tasks	Restore a deleted item from the recycle bin.
`-showtasks`	Recycle Bin tasks	Display information about pending or running recycle bin tasks and actions.
`-startdelete`	Recycle Bin tasks	Start the nightly recycle bin automatic deletion action.
`-startpurge`	Recycle Bin tasks	Start the nightly recycle bin purge action.
`-stopdelete`	Recycle Bin tasks	Stop the nightly recycle bin automatic deletion action.
`-stoppurge`	Recycle Bin tasks	Stop the nightly recycle bin purge action.
`-children`	Schema export	Export children of children as well.
`-class=<c1,c2>`	Schema export	Only export objects of classes in the list (default: all classes).
`-dn=<dn1,dn2>`	Schema export	Only export the DNs in the list (default: \VED\Policy).
`-export=<xmlfile>`	Schema	Export schema to file

Parameter	Type	Description
	export	<xmlfile>.
`-subsys=<IOSCAR>`	Schema export	Only export specified subsystems: ■ `O` - ObjectStore ■ `R` - Rights ■ `I` - Identity ■ `C` - Schema ■ `A` - OAuth ■ `S` - SecretStore (default:OS) Specify one or more subsystems. For example: `-su=ics` or `-su=o` or `-su=oricas`.
`-import=<xmlfile>`	Schema import	Import schema from file <xmlfile>.
`-version`	Schema information	Display the current schema version.

Using the TppPKIs command line tool

The **tpppkis** command-line tool allows you to read and write PKI files. It provides functionality for managing certificates, private keys, CSRs, and PFX files, as well as performing cryptographic operations such as digest creation and HMAC computation.

TPPPKIs tool syntax

The TppPKIs program is located at: `[InstallDir]\Platform\TppPKIs.exe`.

To perform specific tasks, type a parameter directly after typing the `TppPKIs` command. For instance, `tpppkis -help`. Please note that commands and parameters are *not* case-sensitive, meaning `TppPKIs -code` and `tpppkis -code` are interpreted the same.

When running the program with no parameters, you will see the inline help. There, you will see that some characters in parameter names are bolded and some are not. The bolded characters are a short-cut syntax that makes it quicker and easier to type commands. For example, the chain parameter is displayed in the inline help as `-ch`**`ch`**`ain`. The bolded part, in this case `-ch`, is the short cut.

This short-cut syntax can make it quicker and easier to type commands; however, to ensure compatibility with future versions of TppPkis, you should use full parameter names when scripting.

> **TIP** The hyphen (`-`) is technically optional, but is recommended for forwards compatibility.

Command options are additional modifiers that provide further instructions or information to the TppPkis command being executed. For example, -text=<file> is used to load the specified file into PKIX and display a text version. The tool accepts the following operators: `=`, `:`, and ` ` (space). Thus the following examples are all treated the same: `-cr=X509`, `-cr:X509`, and `-cr X509`

Combining these principles, the following commands are all interpreted the same:

```
tpppkis -list all
```

```
tpppkis -LIST=all
```

```
TppPkis -LIst:aLL
```

TppPKIs tool parameters and options

Click a column header to sort by that column.

Option	Type	Description
`-list`	General Options	Lists available options for `<type>`. Available types: `alg`, `all`, `digest`, `key`, `opt`, `priv`, `pub`, `test`, `type`, `usage`.
`-options=o1, o2, oN`	General Options	Sets specific options. Example: `XmlToDo, XmlContainer, GenCmds`.
`-verbose`	General Options	Enables verbose output.
`-der`	General Options	Outputs DER instead of PEM where applicable.

Option	Type	Description
`-xml=file`	General Options	Generates TppTool XML to define objects alongside the regular output.
`-dump=file`	General Options	Decodes the given file and displays it in text form.
`-skip`	General Options	Skips writing transient files created during processing.
`-algorithm=alg`	General Options	Specifies the encryption algorithm for Private Key and PFX files. See `list -alg` for available options.
`-digest=dgst`	General Options	Specifies the digest algorithm to use. See `list -digest` for available options.
`-infile=file`	General Options	Reads commands from a specified file. Each line represents an individual command line.
`-consume=file`	Digest Options	Specifies the file whose contents will be used for creating a digest.
`-hmackey=key`	Digest Options	Specifies the key for HMAC creation.
`-newkey=keytype`	Private key options	Generates a new private key of the specified type. See `list -key` for available types.
`-key=source`	Private key options	Specifies an existing private key source (file path or DN).
`-pass=password`	Private key options	Specifies the password for decrypting the private key file (if required).
`-csr=source`	CSR options	Specifies an existing CSR source (file path or DN).
`-subject=subjectdn`	CSR options	Specifies the subject distinguished name.
`-sandns=d1,d2,...`	CSR options	Specifies SAN DNS names to add.
`-sanip=i1,i2,...`	CSR options	Specifies SAN IP addresses to add.
`-sanrfc822=e1,e2,...`	CSR options	Specifies SAN RFC822 names to add.
`-sanuri=u1,u2,...`	CSR options	Specifies SAN URIs to add.

Option	Type	Description
`-sanupn=u1,u2,...`	CSR options	Specifies SAN UPNs to add.
`-objectsid=sid`	CSR options	Specifies the Microsoft NTDS CA ObjectSID to add.
`-usage=u1,u2,...`	CSR options	Specifies requested key usage. See `list -usage` for available options.
`-cert=source`	Certificate options	Specifies an existing certificate source (file path or DN).
`-serial=number`	Certificate options	Specifies the certificate's serial number.
`-validity=days`	Certificate options	Specifies the number of valid days for the certificate.
`-issuer=source`	Certificate options	Specifies the issuer certificate source (file path or DN).
`-isskey=source`	Certificate options	Specifies the issuer private key source (file path or DN).
`-isspass=password`	Certificate options	Specifies the password for decrypting the issuer private key.
`-selfsign`	Certificate options	Self-signs the certificate.
`-isroot`	Certificate options	Issues the certificate as a Root or Intermediate CA certificate.
`-pfxfile=file`	PFX options	Specifies an existing PFX file.
`-friendly=name`	PFX options	Assigns a friendly name to the certificate.
`-pfxpass=password`	PFX options	Specifies the password for decrypting the PFX file.
`-addcert=source`	PFX options	Specifies additional certificates to add to the PFX (file path or DN).
`-jdktrust`	PFX options	Marks the included certificate as trusted for JDK compatibility.
`-create=type`	Output options	Specifies the type of file to create. Supported types: `PKCS8`, `PKCS10`, `PKCS12`, `X509`, and `Extract`.
`-outfile=file`	Output options	Specifies the output file path.

Option	Type	Description
`-outpass=password`	Output options	Specifies the password for encrypting the output file (if applicable).
`-hsmdll=path`	HSM options	Specifies the cryptoki DLL path.
`-hsmlabel=label`	HSM options	Specifies the partition label.
`-hsmserial=serial`	HSM options	Specifies the partition serial number.
`-hsmpin=pin`	HSM options	Specifies the authentication PIN.
`-hsmtype=type`	HSM options	Specifies the authentication account type (`SO`, `CO`, `0`, `1`).
`-text=file`	Diagnostics options	Loads the specified file into PKIX and displays a text version. Uses `-pass` if specified.
`-chain`	Diagnostics options	Verifies and displays the certificate chain when using `-text`.

Examples

Create a new EC-P256 key and save it as PKCS8

```
tpppkis -create=pkcs8 -newkey=eccp256 -outfile=clear-ecc.pem
```

Encrypt an existing key

```
tpppkis -create=pkcs8 -key=clear-ecc.pem -outfile=enc-ecc.pem -
outpass=badpassword
```

Create a CSR with a new key

```
tpppkis -create=csr -newkey=eccp256 -subject="CN=DemoSystem, O=Bartok, C=US" -
sandns=demosystem.bartok.us,demosystem.bartok.de -usage=clientAuth -
outfile=demosystem
```

Build a certificate authority and issue a certificate

```
tpppkis -create=cert -newkey=eccp521 -subject="CN=CA Certificate" -selfsign -
isroot -
usage=digitalsignature,crlsign,serverauth,clientauth,keyCertSign,keyEncipherm
ent -outfile=ca -der
```

Create a PFX containing a private key and certificate

```
tpppkis -create=pfx -cert=endentity.cer -key=endentity.p8 -outfile=certpluskey
-friendly=bob -addcert=intermediate.cer -addcert=ca.cer
```

8

Trust Protection Platform configuration overview

This section outlines the general configuration requirements that are common to all Venafi Trust Protection Platform™ products.

Use this section to configure your base system.

To complete general Configuration requirements

1. Define your user data stores and identities.

   To manage keys and certificates throughout your environment, Trust Protection Platform allows you to delegate certificate administration to user and group identities. You can use existing users and groups from Active Directory, or you can create users and groups in the local Trust Protection Platform database.

   a. Define users.

      For more information, see "Working with identities, permissions, and teams" on page 635.

   b. (Conditional) If you are using the Local Directory, define the local user and group identities.

      For more information, see "Managing local identities directly in Trust Protection Platform" on page 693.

c. (Conditional) If you are using large AD directories, define search expressions on the AD Connection object's **Search Expression** tab to narrow the object attributes and classes that are searched during a query.

   For more information, see "Filtering identities" on page 740.

   For more information on user administration, see "Working with identities, permissions, and teams" on page 635.

2. Manage administrative permissions for your system objects.

   For information on assigning permissions to objects in Trust Protection Platform, see "Assigning object permissions in the Policy Tree" on page 739.

   For more information on how permissions assignments work in Trust Protection Platform, see "Permissions overview" on page 713.

   For information on viewing an administrator's effective permissions, see "Viewing user entitlements" on page 714.

3. Configure your system folders.

   For more information on creating and deploying folders, see "Using policies to manage encryption assets" on page 859.

4. (Optional)Configure your system encryption keys.

   If you want to use AES encryption keys on a supported HSM device to secure encryption assets stored in the Trust Protection Platform database, see "Managing system encryption keys" on page 545.

5. Set up your logging system.

   For more information, see "Logging overview" on page 416 in the Log Server Administration Guide.

6. Configure the Default SQL Channel object.

   For more information, see "SQL Server channel" on page 443 in the Log Server Administration Guide.

7. Configure the Log View Server setting in the Policy object.

8. Configure your system Channel objects

   For information on defining Channel objects, see "Creating Channel objects" on page 442 in the Log Server Administration Guide.

9. Configure your system Notification Rules.

For information on defining Notification Rules, see "Setting up notification channels" on page 439 in the Log Server Administration Guide.

For more information on system notifications and logging, see "Understanding system logging and notifications" on page 983.

10. Configure your system reporting.

    For information on configuring the Reporting module, see "Configuring the Reporting module" on page 852.

11. Create the Report objects.

    The individual Report objects determine report format, how often the report is generated, and report delivery options. For information on configuring Report objects, see "Managing system reports" on page 977.

12. Implement the Network Discovery components on the Trust Protection Platform server.

    For more information, see Discovering certificates and keys in the Certificate Management Guide.

13. (Conditional) If you are scanning large systems, you can deploy multiple Discovery Servers to load balance or, if you are scanning public and private IPv4 addresses, you can configure one Discovery Server inside the firewall and another outside the firewall.

14. (Conditional) If you have multiple Discovery Servers, you can define the zones you want each Discovery Server to service in the Trust Protection Platform Server object. The Discovery Zones allow you to manage which servers process which discoveries.

15. Configure the Discovery Module in the Platforms tree. The Discovery Module is the component that runs the configured discoveries. The Discovery Module object allows you to define discovery processing times and scan settings.

    For more information, see "Configuring the Discovery module" on page 855.

16. (Conditional)If you want to discover SSH keys or certificates in local file systems or keystores, install and configure the agent.

17. Install the agent on any machine where you want to discover SSH keys (either server or user keys) or certificates in the local file system or keystores.

General configuration options

This section outlines the general configuration options that are common to all Venafi products—Venafi TLS Protect and Venafi SSH Protect. Use this section to configure your base system.

After you configure the base system, you can then refer to the system-specific configuration requirements for your Trust Protection Platform product.

Field	Description
Description	Description for the encryption object.
Contact	User or group Identities assigned to this object.Default system notifications are sent to the contact identities. Default contact = master administrator To select the object contacts: Click the Browse button. The Identity Selector dialog opens. If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, you can enter the wildcard character (*). Select a User or Group Identity, and then click **Select**. Press Shift+click to select multiple, contiguous users and groups. Press Ctrl+click to select multiple, discontiguous users and groups.

Field	Description
General Tab	
Log Tab	Provides a view of all events triggered for the current object. An administrator must have a minimum of the Read permission to view this tab. For more information on the Log tab options, see Viewing log events.
Permissions	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Securing Trust Protection Platform's web servers

To secure and protect all web services created and used by the system, Trust Protection Platform automatically redirects HTTP requests to HTTPS and provides a server certificate. This method ensures that all inbound authentication processes are secure.

During installation, Trust Protection Platform creates a self-signed Venafi Operational Certificate (VOC) for each Venafi server, and places them in the Venafi Operational Certificate folder of the policy tree.

CAUTION You should never use a self-signed certificate in production. The self-signed certificate generated by the Trust Protection Platform server is for convenience in development or test environments only. For production environments, install your own CA-issued certificate. To replace the self-signed certificate, see "Replacing the Venafi Operational Certificate (VOC) with your own CA-signed certificate" on the next page in the *Administration Guide*.

Exceptions to HTTPS Redirects

Because encryption is built into the SCEP protocol used by Network Device Enrollment, SSL/TLS is not enforced like it is for other Venafi web services. This is useful for servicing certificate enrollment requests from legacy SCEP clients that do not support SSL/TLS (HTTPS).

About the Venafi Operational Certificate

Venafi Trust Protection Platform 25.1 uses the Venafi Operational Certificate (VOC) to secure all TLS traffic to the Venafi web server. Once you renew the VOC it will be used the next time the IIS Application Pools refresh.

> **BEST PRACTICE** Delete your current Venafi IIS certificates and associated device and application objects after the upgrade so that you don't have duplicates of the same certificate or set the certificate to use a provisioning driver unnecessarily.

For more information on the VOC, including updating it, see "Replacing the Venafi Operational Certificate (VOC) with your own CA-signed certificate" below.

Replacing the Venafi Operational Certificate (VOC) with your own CA-signed certificate

You should replace the Venafi Operational Certificate (VOC) that secures web services and the Trust Protection Platform log server with your own CA-signed certificate. However, replacing a VOC is slightly different than replacing other certificates. The Venafi IIS web site and the Trust Protection Platform Log server place certificates differently. Therefore, device and application objects are not required in order to place certificates. To ensure that you keep both the web services and the log server secure, refer to the following procedure.

To replace the VOC

1. From the Platform menu bar, click Policy Tree.
2. On the **Policy** tree, expand the **Venafi Operational Certificate** folder and select the VOC certificate.
3. On the **Settings** tab, clear the **Processing Disabled** check box.
4. In the **Management Type** field, select **Enrollment**.
5. If necessary, update the **Common Name** with the Fully Qualified Domain Name (FQDN) of the Trust Protection Platform server.

6. Select an existing **CA Template**. If none apply, create a new Certificate Authority (CA) template. For more information, see Managing certificate authority (CA) templates in the *Certificate Authority and Hosting Platform Integration Guide*.
7. Update any other fields as necessary, and then click **Save**.
8. In the **Platforms** tree, select your Trust Protection Platform engine.
9. On the **Settings** tab, assign the VOC **Certificate**, and then click **Save**.
10. (Optional) If you want the VOC to apply to more than one Trust Protection Platform server, repeat these steps for assigning the VOC to each server.
11. When the VOC certificate enrollment completes, navigate back to the **Policy** tree, expand the **Venafi Operational Certificate** folder, and then select the VOC certificate.
12. Click **Renew Now**.
13. After processing for the certificate completes, perform an IIS Reset on each server to enable the certificate to take effect immediately, or alternatively, the system will automatically provision the certificate at midnight (server time).

    NOTE To ensure any Server Agents have the opportunity to download the new trust bundle, any valid CA issue certificate will not be replaced by the system until two days prior to expiration.

Supporting new Server Agent installation *after* replacing your VOC

If the Server Agent will be installed in your Trust Protection Platform environment *after* the VOC has been replaced, copy the complete chain of the trusted certificate in the Roots tree. Then, update the **Agents should trust these additional issuers when reporting home** field with the new chain.

IMPORTANT Certificates must be formatted using PEM (Base64 OpenSSL).

For more information about the Server Agent, refer to the *Server Agent Installation and Configuration Guide*.

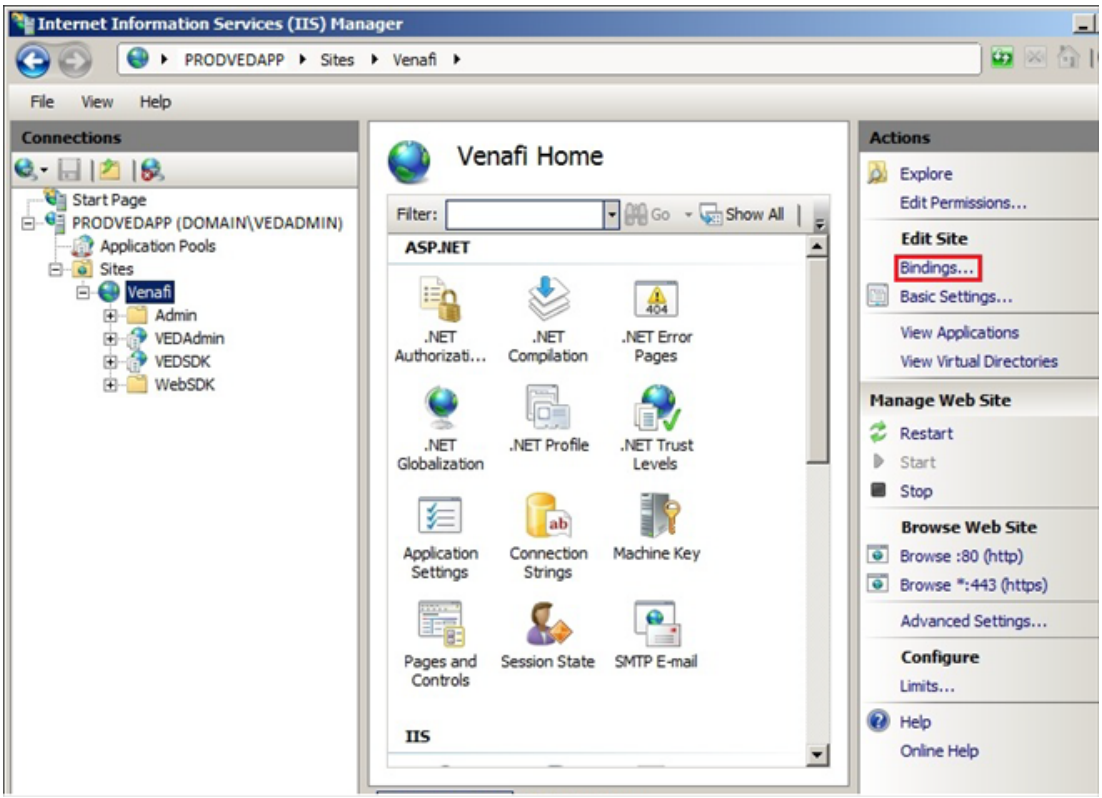
Troubleshooting: manually enabling HTTPS

If for some reason during the installation of Venafi Trust Protection Platform™ the Trust Protection Platform web services are left unsecured–that is, using HTTP and operating without a CA or self-signed certificate–you can manually enable HTTPS and install a server certificate.

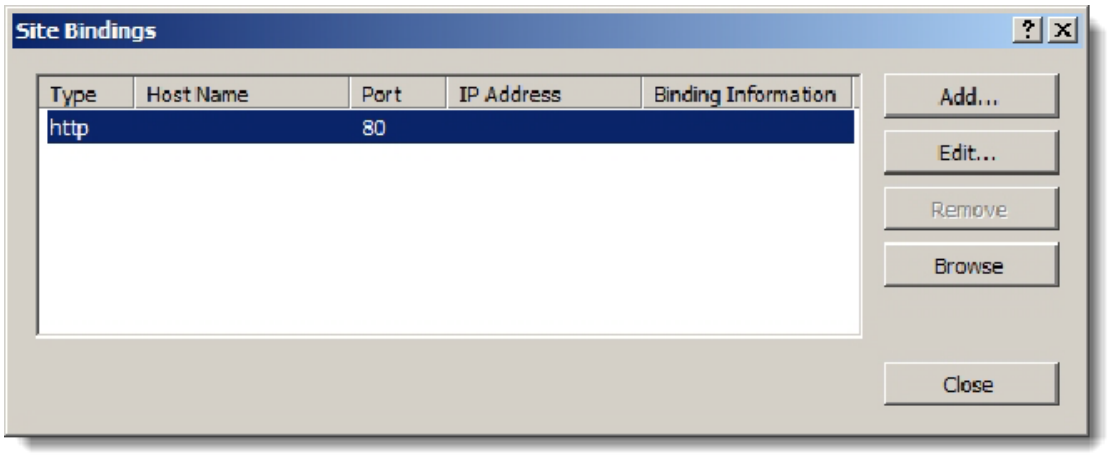
This is especially important in order to secure connections between the Trust Protection Platform server and Server Agents.

To enable the Venafi IIS Web site

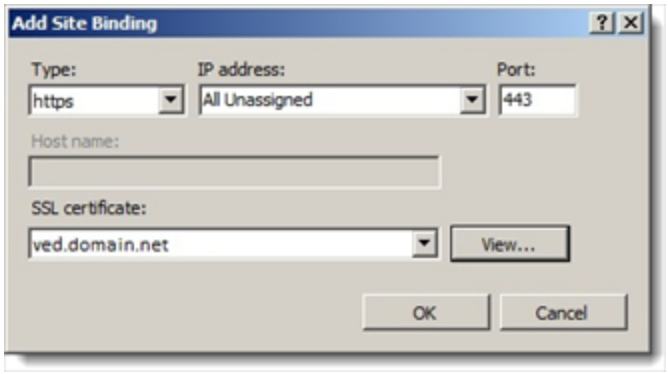
1. In Windows, click **Start**, and then click **Control Panel**.
2. Click **System and Security**, and then click **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Internet Information Services (IIS) Manager**.
4. In IIS Manager's **Connections** pane, expand your server's node, and then expand the **Sites** node.
5. Click the **Venafi** site.
6. In the **Actions** pane, under **Edit Site**, click **Bindings**.



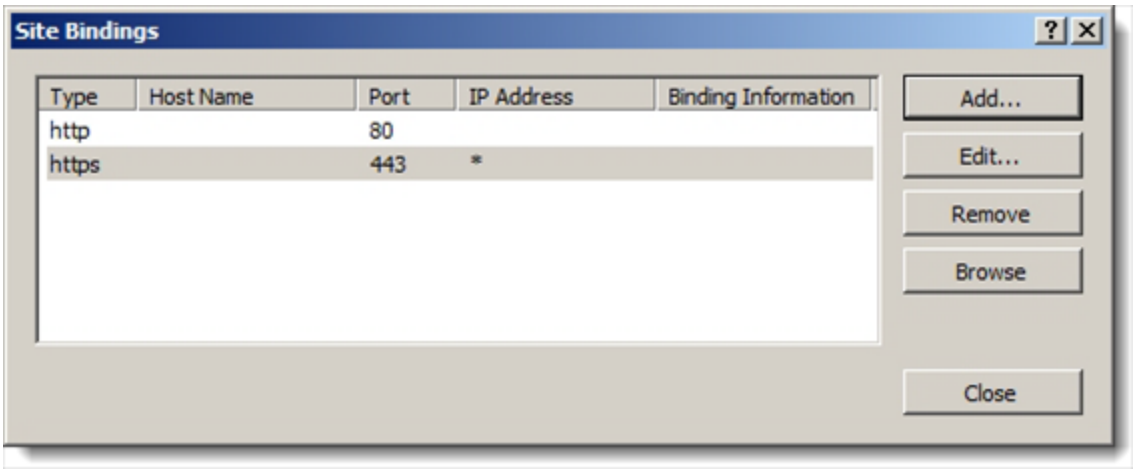
7. In the Site Bindings box, click **Add**.



8. In the **Add Site Binding** box, do the following:
9. Click the **Type** arrow and select **https**.
10. Click the **SSL Certificate** arrow, select the certificate that was provisioned for use by **Trust Protection Platform**, and then click **OK**.



11. When you are finished, click **Close**.



12. Restart IIS.

Supported SSH Ciphers, HMACs, Key Exchanges, and Public Keys

Venafi Platform uses outbound SSH communication for both the TLS Protect and SSH Protect products in the following ways:

TLS Protect uses outbound SSH communication for:

- Agentless Push Provisioning of TLS certificates to target systems
- Onboard Discovery of target systems to find TLS Certificates
- Management of Certificate Trust Stores on target systems
- Daily Installation Validation of TLS certificates to ensure the correct certificate is installed on the expected target system with expected configuration

SSH Protect uses outbound SSH communications for:

- Agentless Discovery of User Private Keys, Server Private Keys, Authorized Key files, and Known Host files
- Agentless rotation of User and Server Private Keys and updating the authorized key and known host files.
- Agentless installation and rotation of SSH Certificates

The available Ciphers, HMACs, Key Exchanges, and Public Keys available to establish a successful SSH connection is dependent upon a number of factors:

- SSH configuration and support of the target system
- Version of Trust Protection Platform
- Do you have Common Criteria Compliant registry values enabled? (See end of this article for more detail)

Category	SSH Identifier	Version Added	CC	General	RFC
Cipher	3des-cbc	< 21.4		✓	
Cipher	aes128-cbc	< 21.4	✓	✓	
Cipher	aes192-cbc	< 21.4		✓	
Cipher	aes256-cbc	< 21.4	✓	✓	
Cipher	3des-ctr	< 21.4		✓	
Cipher	aes128-ctr	< 21.4	✓	✓	RFC 4344
Cipher	aes192-ctr	< 21.4		✓	
Cipher	aes256-ctr	< 21.4	✓	✓	RFC 4344
HMAC	hmac-sha2-256	< 21.4	✓	✓	RFC 6668
HMAC	hmac-sha2-256-etm	22.1		✓	
HMAC	hmac-sha2-384	< 21.4		✓	
HMAC	hmac-sha2-512	< 21.4	✓	✓	RFC 6668
HMAC	hmac-sha2-512-etm	22.1		✓	
HMAC	hmac-sha1	< 21.4	[1]	✓	
Key Exchange	curve25519-sha256	22.1	✓	✓	RFC 8731
Key Exchange	curve25519-sha256@libssh.org	22.1		✓	
Key Exchange	ecdh-sha2-nistp256	22.1	✓	✓	RFC 5656
Key Exchange	ecdh-sha2-nistp384	22.1	✓	✓	RFC 5656
Key Exchange	ecdh-sha2-nistp521	22.1	✓	✓	RFC 5656
Key Exchange	diffie-hellman-group18-sha512	< 21.4	✓	✓	RFC 8268

[1] In versions of Venafi Platform <21.4, hmac-sha1 was enabled in Common Criteria mode. Starting in version 22.1, it has been removed from the Common Criteria list.

Category	SSH Identifier	Version Added	CC	General	RFC
Key Exchange	diffie-hellman-group16-sha512	< 21.4	✓	✓	RFC 8268
Key Exchange	diffie-hellman-group14-sha256	< 21.4	✓	✓	RFC 8268
Key Exchange	diffie-hellman-group14-sha1	< 21.4		✓	
Key Exchange	diffie-hellman-group1-sha1	< 21.4	[1]	✓	
Public Key	ssh-rsa	< 21.4	✓	✓	
Public Key	rsa-sha2-256	22.1	✓	✓	RFC 8332
Public Key	rsa-sha2-512	22.1	✓	✓	RFC 8332
Public Key	ecdsa-sha2-nistp256	< 21.4	✓	✓	RFC 5656
Public Key	ecdsa-sha2-nistp384	< 21.4	✓	✓	RFC 5656
Public Key	ecdsa-sha2-nistp521	< 21.4	✓	✓	RFC 5656
Public Key	ssh-ed25519	< 21.4	✓	✓	RFC 8709

Common Criteria Compliance

To configure Venafi Platform to only use Common Criteria-compliant SSH algorithms for outbound SSH Communication, you must:

- Put the following in a plain text file (using a program like Windows Notepad), and saving as a `*.reg` file

Registry key to force Common Criteria compliance

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Venafi\Platform]
"Common Criteria Compliant"=dword:00000001
```

[1] In versions of Venafi Platform <21.4, diffe-hellman-group14-sha1 was enabled in Common Criteria mode. Starting in version 22.1, it has been removed from the Common Criteria list.

Error scenario

If you see an error message similar to the following, you need to upgrade to Venafi Platform 22.1 (or higher).

> The SSH library failed to connect to {Target System} on port 22, with the Connection Result 9: Failed to negotiate a transport component [diffie-hellman-group14-sha1] [curve25519-sha256]

This message indicates that Venafi Platform could not find an algorithm that was supported by both Venafi Platform and the remote server.,

9

Managing system encryption keys

Venafi Trust Protection Platform™ maintains all system information—that is, configuration settings, managed server and certificate information, credentials, archived certificates and private keys—in a database. To secure this information, Trust Protection Platform uses either a software encryption key or a hardware encryption key on a supported HSM device to encrypt the information used to connect to the database.

To secure the encryption assets within the database, Trust Protection Platform also encrypts sensitive information such as certificate private keys, Credential objects, and SSH keys. Trust Protection Platform uses the encryption key to secure encryption assets within the database.

This chapter contains the following topics:

Overview of encryption drivers 546

Configuring the root encryption driver 549

Database Encryption 551

Managing the default software encryption key 553

Managing the null key 555

Using HSM-protected encryption keys 557
Validating encryption keys 566
Using encryption keys to secure encryption assets 566
Venafi Advanced Key Protect 580

Overview of encryption drivers

The Software and Null Encryption drivers are provided by default when you install or upgrade via the Venafi Configuration Console.

About hardware (HSM) and software encryption

In the past, adding an HSM could only be done after product installation. Now, during a new installation, you can set up a hardware (HSM) encryption key that allows data encryption without requiring a separate software encryption key.

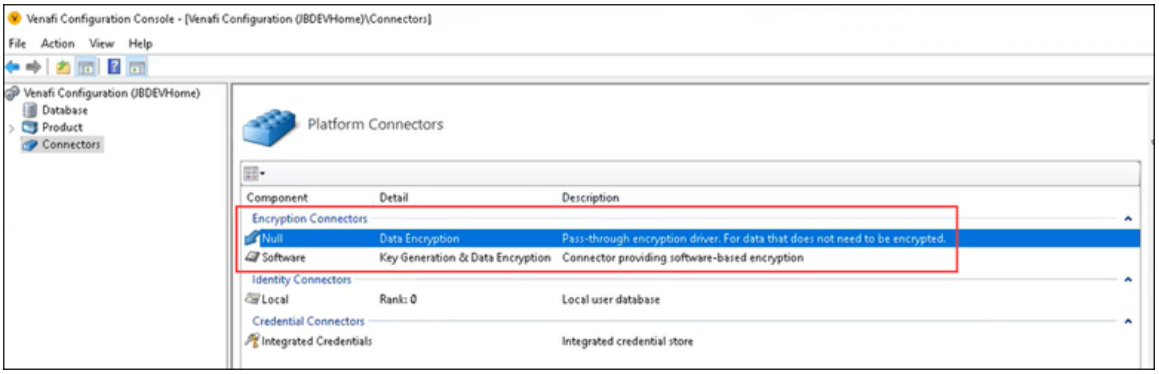
If you **Enable Hardware Encryption**, then you can opt out of enabling a separate software encryption key. In that scenario, software encryption is used for key generation only.



About the Software and Null connectors

The software key is Trust Protection Platform's default encryption key. It is an AES-256 key that is stored in the Windows registry.

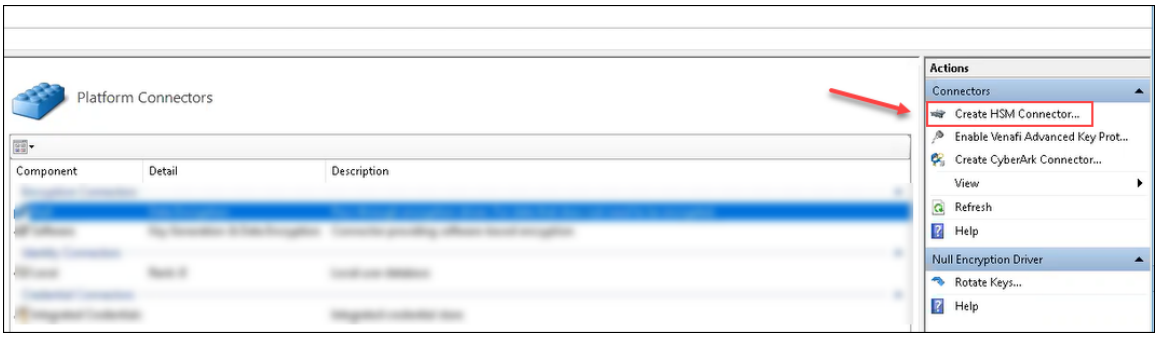
The Null encryption driver actually provides no encryption key at all. It gives users the option of selecting no encryption for objects, such as certificates, that do not need to be secured.



For more information on the default encryption drivers, see "Managing the default software encryption key" on page 553 and "Managing the null key" on page 555.

Creating an HSM connector

If you want to use AES keys stored on a SafeNet Luna SA or Entrust nShield device, or if you want to store code signing keys on those devices, you must first configure the device connection via the "Venafi Configuration Console" on page 44 then create a Hardware Encryption Driver object . For information on configuring an HSM device connection and a Hardware Encryption Driver, see "Using HSM-protected encryption keys" on page 557.



After you configure the device connection and create the Hardware Encryption Driver, you can select the driver's corresponding encryption keys to define your system's default encryption key settings as well as individual Certificate and Credential object encryption keys.

> **NOTE** For more information on defining your system's default encryption keys, see "Using encryption keys to secure encryption assets" on page 566.

How it works

Encryption keys are critical to Trust Protection Platform's functionality. Consequently, during startup, Trust Protection Platform loads every encryption driver and validates its associated encryption keys. If Trust Protection Platform is unable to load an encryption driver or validate any one of the encryption keys, it logs an error to the local Windows system event log and shuts down. You can still run Venafi Configuration Console with reduced functionality so that you can correct the problem; however, the Venafi Trust Protection Platform service itself, will not load until the problem is corrected.

NOTE If the encryption driver fails to initialize at startup, the error message logged to the local Windows system event log is “Encryption driver *driver_name* (DN: *driver_DN*) failed to initialize.” If an encryption key is not valid, the error message is “Encryption key '*driver_name*: *key_name*' is not valid.”

To provide some level of redundancy and system failover, Trust Protection Platform can use the same encryption key from different Encryption Drivers as long as the Encryption key name and password are the same. Moreover, if multiple copies of the same key exist on the HSM device, you can select a copy of the original key as long as it has the same fingerprint as the original.

However, once you initialize a key, you cannot change the encryption key itself. If a configured encryption key is not available or is not valid when Trust Protection Platform attempts to write encrypted data to the Secret Store, Trust Protection Platform logs an error to the local Windows system event log, notifies the user at the administration console, and shuts down.

CAUTION Trust Protection Platform does not back up HSM-protected keys. You must create your own backup of encryption keys stored on an HSM device.

Configuring the root encryption driver

IMPORTANT By default, only Master Administrators can view, edit, or delete Encryption objects in the Encryption tree.

The following table describes the available settings and options for the root Report object.

Field	Description
Encryption Tab	
 Rotate	Allows you to automatically re-encrypt all objects in the tree with the designated encryption key. This action re-encrypts all objects encrypted with the designated key. This includes certificates, private keys, SSH keys, symmetric keys, and all credentials.

Field	Description
	This option allows organizations that already have secrets encrypted with the software key to migrate to an HSM-based key in a single action. Likewise, organizations that must periodically rotate their encryption keys can now do so in a single action. For more information, see "Rotate Secret Store encryption keys" on page 83. While you can rotate keys in the Policy Tree, we recommend you rotate keys in the Venafi Configuration Console.
Default Key Generation	Encryption driver used to generate symmetric or asymmetric key pairs in Trust Protection Platform. When Trust Protection Platform generates the CSR on the server, this global setting determines which encryption driver is used to generate a new key pair. The Generate Key/CSR on Application setting in the Certificate object allows you to determine where the CSR and the private key are generated. For more information on this settings, see Certificate settings in the *Certificate Authority and Hosting Platform Integration Guide*. Not all encryption drivers support key generation in Trust Protection Platform. Only encryption drivers that support key generation are available in the drop-down menu. If you want your SSH keys to be generated on a remote system, this setting must be set to the remote system where all the SSH keys will be generated. If you want to override this for certificates, you can do so via policy.

Field	Description
General Tab	
Log Tab	Provides a view of all events triggered for the current object. An administrator must have a minimum of the Read permission to view this tab. For more information on the Log tab options, see Viewing log events in the *Log Server Administration Guide*.
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Database Encryption

Venafi Platform uses encryption at rest to protect the information stored in your database. There are two options for database encryption: software encryption, and hardware encryption. You must use some combination of the two (hardware, or software, or both).

Understanding your encryption options is important so you know how Venafi Platform is protecting your data.

For more information on encryption drivers and how to configure them, see "Overview of encryption drivers" on page 546.

Software Encryption

If you select software encryption, your database assets will be encrypted using an AES-256 encryption key stored in the Windows registry. You either provide a key, or have Venafi Platform generate a key for you. You must use the same encryption key on all Venafi servers.

To export your software key for backup or to us on another server, you can use the Venafi Configuration Console (VCC), or you can use the command line.

For information on using VCC, see "Backing up the software encryption key" on page 554.

To backup using the command line, run the following command:

```
tppconfiguration.exe -keyexport:<file-path>
```

Hardware Encryption

If you select hardware encryption, your encryption material will be stored on a hardware security module (HSM), such as one provided by SafeNet Luna SA, Entrust nShield, or other HSM provider.

> **NOTE** While most other uses of HSMs require Venafi Advanced Key Protect (AKP), you can encrypt secrets in your database using an HSM without a license for AKP.

More information on hardware encryption can be found at "Using HSM-protected encryption keys" on page 557.

Tips for using both types of encryption

You can use both software and hardware encryption. If you choose to do so, there are some things you should be aware of.

- During a first-time install, you can configure both software and hardware encryption.
- When you install on subsequent servers, you must use the same configuration as the initial installation.
- On subsequent servers, if you only used only one form of encryption, the other encryption screen is disabled, since the system detects it is not required.

Adding software encryption to an existing system

If you install with only hardware encryption, and later go back to add software encryption, there are specific steps to follow because you will have one Venafi server with software encryption and your other servers won't be able to connect to the newly-encrypted database. Follow these steps to apply software encryption to your HSM-protected cluster:

On the first server (it doesn't matter which of your servers you pick):

1. Stop all services.
2. In Venafi Configuration Console (VCC), open **Connectors** > **Software** > **Properties** and enable **Encryption and Key Generation**.
3. Close VCC, then reopen it.

   This procedure triggers the platform to generate a software key.

   Export the new key, using the console, or using the following command line switch:

   ```
   tppconfiguration.exe -keyexport:<file-path>
   ```

4. Restart services.

On all other servers in the cluster:

1. Stop all services.
2. Using the command line, import the key using the following command line switch:

   ```
   tppconfiguration.exe -keyimport:<file-path>
   ```

   For example:

   ```
   tppconfiguration.exe -keyimport:c:\software-key.pem
   ```

   You'll be asked to provide the password for the PEM file, then the key will be imported.
3. Restart all services.

Read more about how to use `tppconfiguration.exe` and associated command line switches at "Using the TppConfiguration command line tool" on page 511.

Managing the default software encryption key

Trust Protection Platform has the ability to encrypt its database with a software encryption key.

IMPORTANT When used, the Venafi Platform software key is critical to Trust Protection Platform's functionality. Without it, Trust Protection Platform cannot access the Trust Protection Platform database. Consequently, it is strongly recommended that you back up the software key to a secure location. In the event of a system failure, you can restore the key so Trust Protection Platform can

access your system data. For information on backing up and restoring the software key, see "Backing up the software encryption key" below.

By default, this same encryption key is used to encrypt certificate private keys, Credential objects, and SSH keys.

You manage the Venafi Platform software key in the Venafi Configuration Console, or through the command line client.

Backing up the software encryption key

When you installed and configured Venafi Trust Protection Platform, you had the option to enable either software or hardware encryption (or both). If you enabled software encryption, you need to back up the software encryption key to a secure location. The software key is critical to the functionality of Trust Protection Platform. Without it, you cannot access data in the database. In the event of a system failure, you will need a copy of the encryption key to access your data. Additionally, if you want to install additional Trust Protection Platform servers, you will need the software key to install and configure those servers.

DID YOU KNOW? How is the Venafi Trust Protection Platform software key used and why is it so important to back it up?

Trust Protection Platform maintains all system information—that is, configuration settings, managed server and certificate information, archived certificates, and private keys—in a database. To secure this information, Trust Protection Platform uses an AES-256 encryption key—the software key—to encrypt the connection to the database.

Depending on the encryption key selected in the object configuration, the objects themselves can be encrypted using the software key. The key is securely stored in the Windows registry.

For more information about why it's important to back up your data, see "Disaster recovery operations" in the Installation and Upgrade Guide.

To export the software key from Venafi Configuration Console

1. From the Venafi Trust Protection Platform server, open **Venafi Configuration Console**.
2. In the left panel, click **Connectors**.
3. In the center panel, click the **Software** component.
4. In the Actions panel on the right, click **Export Key...**

5. (Conditional) If requested, enter the Venafi Platform administrator user name and password.
6. Enter a password to encrypt the exported key.
7. Click **Browse** to select a location to export the key.
8. Click **Export**.

For more information, see "Venafi Configuration Console" on page 44 in the Administration Guide.

To export the software key from the command line

1. On the Venafi server, open a command line and browse to the Venafi installation directory.
2. Run the following command:

```
tppconfiguration.exe -keyexport:<file-path>
```

Managing the null key

The Null encryption driver actually provides no encryption key at all. It gives users the option of selecting no encryption for objects, such as certificates, that do not need to be secured.

> **NOTE** Certificates are public information, so it is not necessary to encrypt them. Encrypting certificates simply adds unnecessary processing overhead and, depending on the number of certificates you have in your system and whether your encryption keys are stored on an HSM device, may slow your system.

The Null Encryption Driver is provided by default in the Encryption tree.

Field	Description
Description	Description for the encryption object.
Contact	User or group Identities assigned to this object.Default system notifications are sent to the contact identities. Default contact = master administrator To select the object contacts:

Field	Description
	Click the Browse button. The Identity Selector dialog opens. If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, you can enter the wildcard character (*). Select a User or Group Identity, and then click **Select**. Press Shift+click to select multiple, contiguous users and groups. Press Ctrl+click to select multiple, discontiguous users and groups.

General Tab

Log Tab	Provides a view of all events triggered for the current object. An administrator must have a minimum of the Read permission to view this tab. For more information on the Log tab options, see Viewing log events.
Permissions	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Using HSM-protected encryption keys

In connection with (or as an alternative to) the Venafi Platform software key, Trust Protection Platform allows you to use AES encryption keys stored on supported and compatible hardware security modules (HSMs).

An HSM is a dedicated, physical device designed to securely manage, process, store, and even generate cryptographic keys. HSMs are used to enhance the security of sensitive data and cryptographic operations in many industries.

Key characteristics and functions of an HSM include:

- Secure key management
- Safe cryptographic operations
- Tamper resistance
- Compliance and certification with industry standards
- Access controls
- Backup and recovery

HSMs are specialized devices that provide a secure environment for cryptographic operations and key management, significantly enhancing the security posture of any organization that handles sensitive data and transactions.

An HSM must be properly connected to each server in the cluster. Connection information between the server and the HSM is stored in encrypted format in the server's Windows Registry as well as in the database's Secret Store. When you make changes (In VCC) to the HSM configuration settings, the changes are communicated to all other servers in the cluster, which will update their own Windows Registry settings with the updated information. Thus, changes to HSM configuration settings don't need to be repeated on all servers in the cluster.

IMPORTANT If you elect to use a hardware security module (HSM) to protect your assets in Trust Protection Platform, you must ensure that you use your HSM vendor's documented method to back up the keys. In addition, if you use Venafi Platform software encryption, you should ensure the software key is backed up. For information on backing up the software key, see "Backing up the software encryption key" on page 554.

What's next?

- If you want to learn about remote vs central key generation, look at "Supported methods of key generation" on page 581, then you may want to review "Hardware central key generation with Venafi Advanced Key Protect" on page 585 and "Hardware remote key generation with Venafi Advanced Key Protect" on page 588.
- Do you need to pick an HSM vendor? Look at Supported HSMs in our System Requirements to see which HSMs are supported and which HSMs are compatible with Trust Protection Platform.
- Are you ready to connect Trust Protection Platform to an HSM? You're going to need the vendor's documentation, but we've got an overview of the process in "HSM Configuration" below.
- Are you wondering about how to create an HSM connector in VCC? You'll find that in "Creating a HSM connector" on page 562. Don't forget to enable it in Policy Tree once the HSM software has been installed and tested on all servers in the cluster.

HSM Configuration

Installing a Hardware Security Module (HSM) on your server is a multi-step process that ensures your cryptographic operations are secure. While the specific steps may vary depending on the HSM vendor, the following general instructions provide an overview of the typical process.

> **CAUTION** Using an HSM-protected key requires proper configuration, backup, and consistent uptime of the HSM for Trust Protection Platform to operate. If no HSM device is available, Trust Protection Platform attempts to reconnect to the HSM for a period of time, then it logs an error to the local Windows system event log and shuts down. If a broken HSM connection causes Trust Protection Platform to shut down, you will need to use VCC to update the HSM settings. The Venafi Trust Protection Platform service itself will not load until the problem is corrected and the connection is reinitialized.

For a list of supported HSM versions with links to their documentation (when available), see Supported HSMs in the System Requirements. Be aware that Azure Dedicated HSMs are powered by SafeNet Luna SA, so they are supported, and should be configured using SafeNet Luna SA instructions.

You will likely need to refer to the vendor's documentation when installing and configuring the HSM and client software.

Venafi provides support only for *supported* HSMs. If you need assistance with a *self-certified* HSM, please contact the vendor directly.

IMPORTANT HSM connectors are global configurations. As such, the following requirements must be met before your begin:

- All Trust Protection Platform servers need to have access to the HSM.
- The HSM client must be installed to the same location on all Trust Protection Platform servers.
- The HSM client must present the same partition label on all Trust Protection Platform servers.
- Ideally the serial number presented for the partition is the same on all servers.

Make sure all of these requirements are met before creating an HSM connector.

Once these requirements are met for every Trust Protection Platform server in the cluster, you can then create a connector to the HSM from any server in the cluster.

Since HSM connectors are global configurations, each server in the cluster will load the configuration after it is created on one of them. HSM information is stored in encrypted form in the registry (only when the System Protection Key is stored in the HSM), and in Secret Store. When it is updated in VCC, the updates are stored and VCC passes the information to other servers in the cluster. If the System Protection Key is on the HSM, the individual Venafi servers will update their registries.

TIP When using an HSM setup, we strongly recommend you use a High Availability (HA) setup, which will ensure redundancy in the HSM environment. This means that if one HSM in the HSM HA setup goes down (maintenance, hardware error, etc.), Trust Protection Platform will still function. We recommend you review your HSM vendor's documentation for information about their HA offerings.

Prerequisites

1. **Review Documentation.** Obtain and review the installation and configuration documentation provided by your HSM vendor. Links to vendor documentation are provided, when available, in the Supported HSMs section of the System Requirements.
2. **Verify Compatibility.**: Ensure your server hardware, operating system, and software are compatible with the HSM.
3. **Backup Data.** Perform a full backup of your server to prevent data loss during installation.

Installation Steps

1. Install HSM Drivers and Software:
    - Obtain the latest HSM drivers and management software from the vendor's website or installation media.
    - Follow the vendor's instructions to install the client drivers on each server in the cluster.
    - Use the vendor-provided management software to initialize and configure the HSM client on each server in the cluster.
    - Reboot the servers (if required).
2. Integrate with Venafi Platform:
    - If you don't already have an HSM connector, create an HSM connector using Venafi Configuration Console (VCC).
    - In **Policy Tree**, on the **Policy** root node, click the **Certificate** tab. In the **Other Information** section, select your connector in the **Encryption Key** field.
    - Test the integration to ensure that applications are correctly communicating with the HSM.
3. Verify and Test:
    - Perform initial tests to verify the HSM installation and configuration.
    - Use vendor-provided tools to run diagnostics and confirm the HSM is functioning correctly.
    - Open Venafi Platform on the web. If the HSM is correctly configured, Venafi Platform will function normally.

Post-Installation Steps

1. **Document the configuration**. Record the HSM configuration settings, including administrative accounts, access controls, and key management details.
2. **Implement Monitoring and Alerts**. Set up monitoring tools to keep track of the HSM's performance and status. Configure alerts for any potential issues.
3. **Regular Maintenance**. Follow the vendor's guidelines for regular maintenance, firmware updates, and periodic security audits.

By following these general instructions, you can ensure a smooth installation process for your HSM. Always refer to the specific documentation provided by your HSM vendor for detailed and accurate guidance.

Removing an HSM

Before you remove an HSM from your cluster, you need to make sure all objects that reference the HSM have been removed.

If you attempt to remove an HSM that is being referenced by objects, you'll see a warning box with information on what you need to do to proceed.

Click the **Copy details to clipboard** link to copy a detailed list of objects that are referencing the HSM. Once there are no more objects referencing an HSM, it can be deleted from the cluster.

To delete an HSM

1. Open the Venafi Configuration Console.
2. Open the **Connectors** node.
3. Click the HSM in the **Platform Connectors** panel.
4. Click the **Delete** action in the **Actions** panel.

AWS CloudHSM configuration requirements

Trust Protection Platform supports key storage on AWS CloudHSM for use with CodeSign Protect. Trust Protection Platform also supports database encryption for the Trust Protection Platform SQL database.

> **NOTE** Advanced Key Protect is required to connect Trust Protection Platform to an HSM.

Configure the AWS CloudHSM cluster-id

To ensure seamless failover between HSM devices in your cluster, it is best to identify the HSM Cluster using the **cluster-id**. Using the **cluster-id** ensures the client is aware of all HSMs in the cluster. Currently, you need to manually edit the **cloudhsm-pkcs11.cfg** configuration file to handle the **cluster-id** option.

1. Open **C:\programdata\amazon\cloudhsm\data\cloudhsm-pkcs11.cfg** in a text editor.
2. Add this line before servers:

   ```
   "cluster_id":"cluster-fly6hbn7zog"
   ```

   using your cluster-id number.

IMPORTANT Because the **configure-pkcs11.exe** command does not handle the **-cluster-id** option, any other changes made by **configure-pkcs11.exe** will remove the above line.

By default, the client will not allow a key to be used unless there are two or more HSMs in the cluster. If you want to run only one HSM for testing, then run the following command:

```
configure-pkcs11.exe --disable-key-availability-check
```

Keep in mind the important note above.

What's Next?

- To set up CodeSign Protect to use keys stored on AWS CloudHSM, follow the steps in Setting up CodeSign Protect to use HSM keys.
- See the AWS CloudHSM PKCS #11 documentation for more information on AWS CloudHSM.

Creating a HSM connector

After you have completed the necessary preconfiguration requirements, you can create the HSM connector in the Venafi Configuration Console. The HSM connector provides the information required to access encryption keys in Trust Protection Platform. Trust Protection Platform supports HSM connectors using the PKCS#11 standard using the Cryptoki API.

To create an HSM connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console**, and open the **Connectors** node.
2. In the Actions panel, click **Create HSM Connector**.
3. (Conditional) If requested, enter your Venafi Trust Protection Platform administration credentials.

4. Enter data into the fields, as described below.

Field	Description
Name	Name of the HSM connector. Use something descriptive so you can identify it later.
Cryptoki DLL Path	Trust Protection Platform requires access to the 64-bit version of Cryptoki DLL. For SafeNet Luna SA devices, this is the path to the `cryptoki.dll` file. For Entrust nShield Connect HSM devices, this is the path to the `cknfast.dll` file. After selecting the DLL, click **Load Slots**. Trust Protection Platform will query the HSM and return the available slots. **IMPORTANT** Trust Protection Platform requires the path to the DLL file to initialize the connection to the HSM device. This path will be used for all Trust Protection Platform servers in the cluster (connected to the same database). All servers in the cluster must have their DLL file in the same location.
Slot	Slot ID for the HSM partition where you want Trust Protection Platform to access the encryption keys. **NOTE** While slot numbers are listed in the drop-down list, Trust Protection Platform does not depend on slot numbers. Trust Protection Platform identifies HSM partitions by label first, and in the case that there are duplicate labels, it falls back to the serial number.
User Type	User type required to access the HSM keys on the designated partition (Slot ID). The designated User Type must have sufficient permissions to use the keys in the Encryption Driver's Permitted Keys list.
Pin	Pin, if one is required to access the HSM. If you use Entrust nShield token protection, leave the field empty. If you are setting up AWS CloudHSM, the pin must be in the following format: `<CU_user_name>:<password>`.

Field	Description
Permitted Keys	A list of keys that can be used for encryption and decryption of data by the Trust Protection Platform servers. The keys listed are the ones that can be used to encrypt data stored in the Trust Protection Platform Secret Store.
Allow Key Storage	Tells Trust Protection Platform whether this HSM can be used to generate and store new private keys associated with Code Signing certificates. **NOTE** This feature is available only for Venafi CodeSign Protect and requires Venafi Advanced Key Protect.
New Key (button)	If you want to generate a new AES 256-bit symmetric key on the HSM, click this button. A new key will be generated.

5. Click **Verify**.

These steps only create the connecter that exists between Venafi Platform and the HSM. You will need to use Policy Tree to enable the connector when you are ready. You will do that In **Policy Tree**, on the **Policy** root node. Click the **Certificate** tab. In the **Other Information** section, select your connector in the **Encryption Key** field.

WARNING! Don't change the Encryption Key field in the Policy Tree until the HSM configuration is installed on, and has been tested on every server in your cluster.

Once the HSM connector has been added and the connection has been verified, we recommend reviewing the post-installation steps.

Enabling HSM connection debugging

From time to time there are issues when talking to an HSM which cannot be easily explained. One of the methods for troubleshooting is to enable the HSM client debug logging.

With some HSM vendors the act of enabling debug logging is more involved than others. For example, in order to enable debug logging with a Luna HSM client you need to point to a completely different client assembly. In this scenario, you would need to modify VCC settings for the HSM connector, and this global setting impacts all servers in the cluster.

Venafi Platform provides built-in debugging capability in the Keystore layer. This provides a universal log of the PKCS11 communication that occurs between Venafi Platform and the HSM.

This debugging feature is intended for short-term use in a non-production environment. You should only enable it long enough to get the data you need to resolve your connection issue. You should then disable it.

To enable HSM connection debugging, you will need to edit the registry on one of your Venafi Platform servers.

To enable HSM connection debugging

1. Using a remote desktop tool, connect to the Venafi Platform server desktop.
2. Launch `regedit.exe`.
3. Navigate to `HKLM\SOFTWARE\Venafi\Platform`.
4. Right-click on the Platform folder, and click **New** > **String Value**.
5. Enter the following for the Name:

   `Cryptoki Trace File`
6. Double click the string value you just added, and in the **Value data** field, enter the path and filename where you want the log file saved.

   For example, you could enter something like this:

   `C:\HSM-logs\trace.log`

   CAUTION This directory must already exist or the log entries will not be generated.
7. Restart the service you are trying to troubleshoot.
8. Take the steps to reproduce the issue you are trying to resolve.

   NOTE You will see new Warnings in the Windows Event Log informing you that this registry setting is for troubleshooting and should not be used in a production system.
9. One log file per process will be created in the file location you specified in the registry setting.

IMPORTANT Once you have resolved your issue, be sure to remove the registry key.

To disable HSM connection debugging

1. Using a remote desktop tool, connect to the Venafi Platform server desktop.
2. Launch `regedit.exe`.
3. Navigate to `HKLM\SOFTWARE\Venafi\Platform`.

4. Delete the following value:

   `Cryptoki Trace File`

5. Restart the service you are troubleshooting.

Validating encryption keys

When a user moves a key from the Available Keys list to the Permitted Keys list, Trust Protection Platform encrypts sample data with the key, then stores the encrypted information in the Trust Protection Platform database. Every Permitted Key is associated with one piece of encrypted test data.

The encrypted test data is used at start-up to verify that the key is valid. Trust Protection Platform first uses the key to decrypt the test data, then compares the test data with the original sample. If the samples do not match, the key fails the validation test. Trust Protection Platform logs an error to the local Windows system event log and shuts down

> **NOTE** If an encryption key is not valid, the error message logged to the local Windows system event log is “Encryption key '*driver_name*: *key_name*' is not valid.”

The validation process is also repeated anytime a user clicks the Test & Load Keys option or saves changes in an Encryption Driver object.

Using encryption keys to secure encryption assets

Every SSH key, private key, and Credential object in the Trust Protection Platform database is secured with an encryption key. In Policy Tree, you can manage which encryption keys are used to secure which types of encryption assets.

Understanding cryptographic algorithms in Venafi Trust Protection Platform

Introduction to machine identity security

In modern enterprise environments, machines—including servers, containers, applications, and cloud workloads—interact far more frequently than users do. These machines require unique identities to authenticate securely, establish trust, and protect data. Machine identity security refers to the systems and practices used to manage and protect the digital credentials that enable this trust.

Without effective machine identity security, organizations face serious risks:

- Outages due to expired certificates
- Unauthorized access from orphaned or improperly managed SSH keys
- Compromise of software integrity through misuse of code signing credentials
- Compliance violations due to weak or outdated cryptography

Machine identities are foundational to securing both internal systems and external-facing services. If you are new to this topic, here are some key concepts that will help you understand how Trust Protection Platform helps protect your network.

- Machine identities use cryptographic keys and certificates.
- TLS certificates identify trusted machines through trusted relationships.
- SSH keys and certificates also identify trusted machines.
- Code signing allows you to trust that code hasn't been changed since it was packaged.
- Cryptographic algorithms serve different purposes.
- Algorithm choice impacts machine identity security.
- Central management of machine identities protects your network and ensures trusted communication.

Each of these key concepts is described in more detail in the sections that follow.

Machine identities use cryptographic keys and certificates

Machine identities establish trust between systems. The most common machine identity types include:

- **TLS certificates**: Used to authenticate web servers, APIs, containers, and other systems to clients or other machines. TLS certificates are used to establish trust for the TLS handshake.
- **Code signing certificates**: Used to prove that a document, application, or other digital data originated from a trusted source and has not been modified.
- **SSH keys and certificates**: Used for remote access and automation, often between development tools and systems, or between machines.

Each of these cryptographic assets uses asymmetric cryptography. A private key must remain secure and should never leave the system that owns it. A certificate (or public key, if no certificate is involved) is intended to be distributed and used by others to authenticate the holder of the private key.

To ensure trust is never broken, machine identities have a lifecycle. A key must not be used for longer than a specified validity period to protect against brute-force (and other) attacks. Keys need to be tracked to determine when they need to be rotated and when certificates expire. A certificate must be revoked in case of key compromise (trust is broken on purpose).

Without a system to manage these assets, organizations risk outages, vulnerabilities, and unauthorized access.

TLS certificates identify trusted machines through trusted relationships

A TLS certificate proves to a client that a machine—usually a server or service endpoint—is the correct entity. A Certificate Authority (CA) is used to validate an entity and to issue a certificate. A client that trusts the CA will therefore trust a certificate issued by the CA.

A certificate can contain information about the server or service endpoint, including at least a validity period, information about the entity like its locality and name, the service or server name, and the public key.

When a client connects to a server over HTTPS (or any other TLS-enabled protocol), it checks to see if the certificate:

- Was issued by a trusted certificate authority (CA)
- Is currently valid (not expired or revoked)
- Matches the domain of the server or service
- Uses cryptography that meets with current security standards

If these checks fail, the client refuses to trust the server.

Because TLS certificates are often deployed across many systems and environments, managing them at scale introduces additional complexity. Expired certificates can cause outages. Certificates using deprecated algorithms (like SHA-1) can introduce vulnerabilities. Venafi TLS Protect helps organizations discover, manage, and renew these certificates securely and automatically.

SSH keys and certificates also identify trusted machines

SSH (Secure Shell) is commonly used for remote administration and automation between systems. Unlike TLS certificates, SSH does not rely on a certificate authority. Instead, mutual trust is established by first exchanging public keys.

Each SSH key pair consists of:

- **A public key**, which is copied to machines where holders of the private key should be permitted access.
- **A private key**, which must be kept secure by the user or system initiating the connection.

When a system initiates an SSH connection to another system, it acts as the SSH client, and the target system acts as the SSH server. The client verifies the server's identity by checking the server's public key against entries in the client's `known_hosts` file. If the key matches, the server checks whether the client's public key is listed in the server's `authorized_keys` file. If the client proves ownership of the corresponding private key, access is granted without requiring a password.

SSH keys are powerful, but unmanaged key sprawl is a major security risk. Keys can be duplicated, reused, or left behind when employees change roles or leave the company. Without visibility or policy enforcement, it's difficult to know which keys are valid or necessary.

Venafi SSH Protect helps discover and analyze trusted keys across systems. It enables organizations to audit access, remove unused or unauthorized keys, and ensure that only approved cryptographic algorithms and key sizes are used. Like with TLS certificates, organizations can rotate keys as needed to protect against brute force attacks or compromised keys.

Code signing enables you to trust that digital assets have not been changed

Code signing validates that a document, application, or other digital data originated from a trusted source and has not been modified. When an asset is signed, a digital signature is applied using a private key. Recipients can use the corresponding public key to verify:

- The asset came from a known, trusted publisher.
- The asset has not been modified since it was signed.

Signed assets include applications, documents, scripts, drivers, container images, and more. Most modern operating systems and platforms display warnings or block an asset that is unsigned, signed but altered, or signed by an untrusted party.

If a code signing private key is misused or stolen, attackers can distribute malicious assets that appear legitimate. This risk is amplified in supply chain attacks where compromised software affects downstream users.

Venafi CodeSign Protect secures and governs code signing keys (whether secured by CodeSign Protect or a supported HSM), enabling you to implement approval workflows, and audit all signing activity. These capabilities help prevent misuse and enforce compliance. Like with TLS certificates and SSH keys, organizations can rotate code signing keys as needed to protect against brute force attacks or compromised keys.

Cryptographic algorithms serve different purposes

Machine identities use a variety of cryptographic algorithms, each used for a specific function. The following types of cryptographic algorithms are commonly used in machine identity systems:

- **Asymmetric algorithms** support identity verification and digital signatures. These algorithms are most commonly used for certificate issuance and code signing applications. Common algorithms include RSA, Elliptic Curve, and ED25519, among many others.

  Asymmetric encryption uses a pair of keys, a private key to sign data, and a public key to verify a signature. In the case of SSH, the public key is immediately available. In the case of TLS, the public key comes from a certificate.

- **Symmetric encryption algorithms** are used for encrypting data in transit or at rest. Common algorithms include AES, among many others.

  Symmetric encryption uses the same key for both encryption and decryption, which is why in the case of data in transit, after establishing trust via asymmetric encryption, messages between machines use symmetric encryption.

- **Hash functions**, such as SHA-256, generate fixed-length digests used in signatures and integrity checks.

  Hashing is a widely-used method for verifying data integrity. A hash function converts arbitrary data into a fixed-length string (a hash) that is unique to the original data. Hashing algorithms include SHA2 and SHA3.

  Hashing algorithms are used to reduce the amount of data to be signed. Instead of signing the actual digital asset, they creating a hash of the asset and then sign the hash.

  Hashing is irreversible—you cannot obtain the source data from a hash. A hash (sometimes also called a *digest*) is like a unique digital fingerprint for any piece of data.

- **Quantum-safe algorithms** (also known as Post-Quantum Cryptography or PQC) are designed to resist attacks that would only be possible on a quantum computer. Quantum computers are expected to eventually break traditional public-key systems like RSA and elliptic curve (EC) cryptography using Shor's algorithm. In contrast, quantum-safe algorithms are based on complex mathematical problems—such as lattice-based or multivariate polynomial equations—that are *believed* to be resistant to quantum attacks.

  While quantum computing poses future challenges to public-key cryptography, symmetric encryption and hash functions remain secure due to the longer key and hash lengths in use today.

Research on quantum-safe algorithms is ongoing, and standards in this area are still evolving. Venafi already supports—and will continue to develop support for—quantum-safe cryptography to help customers prepare for the quantum future.

One of the most urgent concerns in post-quantum cryptography is the risk of "harvest now, decrypt later" attacks, in which encrypted data is collected today and stored for future decryption using quantum computers. Organizations can mitigate this risk by adopting quantum-safe algorithms proactively.

One approach to ensuring compatibility and security during the transition to post-quantum cryptography is to use composite digital signatures, which combine a classical cryptographic algorithm with a post-quantum algorithm in a single signature structure. This method is described in the Internet Engineering Task Force (IETF) draft specification Post-Quantum Composite Signatures, published by the LAMPS working group. The draft outlines how to create and validate digital signatures that incorporate both legacy and quantum-resistant algorithms, providing cryptographic agility and helping organizations maintain long-term data security.

Composite algorithm standards are actively under development. The ISO/IEC 14888-4 specification defines how to generate and validate digital signatures that incorporate multiple algorithms. Although this specification has not yet been finalized, it represents a key step in global standardization efforts.

Beginning with version 25.1, Trust Protection Platform includes support for several composite algorithms. Because standards are still evolving, some algorithms supported today may be deprecated in the future if they are not included in the final standards.

Each algorithm offers different performance and security trade-offs.

> **TIP** For a list of encryption types supported by Venafi Platform, see "Algorithm types supported by Venafi Platform" on the next page which includes a filterable and searchable table with details on the algorithm's type, purpose, and security strength.

Algorithm choice impacts machine identity security

Using outdated or weak algorithms can undermine the security of a machine identity. Common risks include:

- Deprecated algorithms, such as SHA-1 or MD5, are vulnerable to collision or forgery attacks.
- Short key lengths, such as 1024-bit RSA, are no longer considered secure and can be brute-forced with modern computing power.

Organizations should adopt and enforce algorithm standards, such as:

- RSA keys with a minimum length of 2048 bits
- EC keys with a minimum length of 256 bits
- SHA2 (SHA-256 or stronger) for all digital signatures

Trust Protection Platform allows you to define cryptographic policy, discover non-compliant certificates or keys, and remediate them through automated replacement.

Central machine identity management protects your network and ensures trusted communication

As environments grow more complex, manual certificate and key management becomes unsustainable. Without centralized control, machine identities may:

- Expire unexpectedly, causing outages.
- Use non-compliant or outdated algorithms or key sizes.
- Persist after they are no longer needed, increasing attack surface.

Centralized machine identity security provides:

- Visibility into where keys and certificates are deployed and how they are used.
- Automation to handle rotation, renewal, replacement, and revocation at scale.
- Policy enforcement to ensure all identities meet organizational and regulatory standards.
- Auditing and reporting to support compliance and incident response.

Venafi Trust Protection Platform delivers centralized lifecycle management across TLS certificates, SSH keys and certificates, and code signing keys and certificates. It enables organizations to operate securely, meet regulatory requirements, and maintain trust across machine-to-machine communication.

Algorithm types supported by Venafi Platform

In the online version of this topic, you can see a table with a complete list of algorithms supported by Trust Protection Platform. The table is filterable and searchable, and due to these features, and its length, it is not reproduced in this PDF version of this guide. We invite you to view the table online in our documentation portal at https://docs.venafi.com/current/supported-algorithms.

About default algorithm configuration

Cryptographic algorithms define the security of keys and certificates used across your organization. Venafi Platform supports a comprehensive list of algorithms, but not all may align with your organization's security policies or compliance requirements. The Default Algorithm Configuration window in Venafi Configuration Console (VCC) allows you to specify which algorithms can be used and in what order of priority.

How default algorithm configuration works

Venafi Platform maintains two categories of algorithms:

- **Available algorithms:** These algorithms exist within the system but are not approved for use. These are the items on the left panel.
- **Allowed algorithms:** These algorithms are authorized globally for use and prioritized according to your organization's security policies. These are the items on the right panel.

By configuring allowed algorithms, administrators can enforce security standards, restrict outdated or vulnerable algorithms, and prioritize stronger cryptographic options.

Why priority matters

Usually, a requester will select the algorithm they want to use from among those allowed by the system, or by policy. However, suppose a certificate is using RSA 1024 when it is allowed by the system administrators. Later, RSA 1024 is removed from the allowed algorithms. When that certificate is renewed, it can't be renewed using RSA 1024, as it isn't permitted anymore, therefore, the system will use the highest-priority allowed algorithm (the highest one in the allowed list that is allowed by policy) to renew the certificate.

It is important to keep your allowed algorithms ranked from highest priority to lowest priority so the system uses the desired fall back algorithm when a previously-used algorithm is no longer allowed.

You can configure priority using the steps described in "Configuring allowed algorithms" on the next page.

Further restriction of algorithms by policy

Sometimes, you will want to restrict individual containers to only allow a subset of the globally-allowed algorithms. In versions of Trust Protection Platform *before* 25.1, you could only enforce a single algorithm by policy, not allow a choice of algorithms. Now you can select multiple algorithms that are allowed by policy, as long as they are on the globally allowed list from VCC (as discussed above). You can even further restrict sub-folders to only use a subset of the algorithms allowed by a higher-level policy setting.

EXAMPLE Suppose you have a container (folder) for certificates issued for devices in Europe, and you have a sub-container (or sub-folder) for certificates issued for devices in Bulgaria.

Your system administrator may have chosen 15 algorithms that are allowed globally in VCC. You can limit the algorithms used for items in the Europe folder to just ten of those globally-allowed algorithms, and you can limit the algorithms allowed for items in the Bulgaria folder to just five of the ten algorithms permitted in Europe.

Venafi Platform provides enhanced flexibility to your policy owners to allow any or all the algorithms available to them, based on the global and parent policy settings.

Using the SDK to manage algorithms

An authorized user of the Venafi's API can use our Algorithm Selector APIs to perform a number of tasks, including setting globally allowed algorithms (instead of using VCC), and setting the allowed algorithms for a container (folder). For more information, see the following OpenAPI endpoint documentation (and related endpoints in the Algorithm Selector section): Get All Algorithms.[1]

Configuring allowed algorithms

Venafi Platform supports many algorithms[2]. As a system administrator, you can define which algorithms your organization can track and use at the platform level, and set their priority. Policies can further restrict allowed algorithms, if needed.

By default, Venafi Platform has enabled all but the most insecure algorithms. When your administrator installed Venafi Platform, they had the option to change those default settings. If you find they need further refinement, a system administrator can make future changes in Venafi Configuration Console (VCC).

To configure allowed algorithms in VCC

1. In Venafi Configuration Console, under the root node, go to the **Actions** panel and click **Configure Allowed Algorithms**.
2. If prompted, enter the local master administrator credentials.
3. In the **Default Algorithm Configuration** window, adjust the allowed algorithms:

[1]View online at: https://docs.venafi.com/Docs/currentAPI/ then search for pkix
[2]For a comprehensive list, see "Algorithm types supported by Venafi Platform" on page 572.

- Use the left and right arrows to add or remove algorithms.
- Use the up and down arrows to change the priority of allowed algorithms.

4. Click **Apply** to save your changes.

For additional information, see "About default algorithm configuration" on page 573.

Managing encryption keys in the Policy tree

In the Policy tree, object encryption is managed via policy. In the Policy object configuration, you can determine which encryption keys are used to secure which types of objects. For example, in the Policy object's SSH User Key tab, you can select the encryption key used to secure the policy's subordinate SSH User keys. Likewise, in the Policy object Certificate tab, you can select the encryption key used to secure the private keys associated with the policy's subordinate Certificate objects.

IMPORTANT The Default Encryption Key settings in the Policy object apply only to subordinate objects in the Policy tree. To define default values for Credential objects in the Credentials tree, you must define the Default Encryption Key settings in the Root Credential object. For more information, see "Managing encryption keys in the Credentials Tree" on page 577.

The following two sections review how to manage encryption keys in the Policy tree.

To Assign Encryption Keys to Specific Types of Objects in the Policy Tree

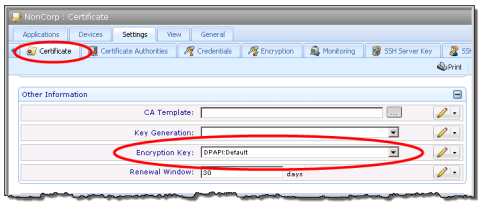
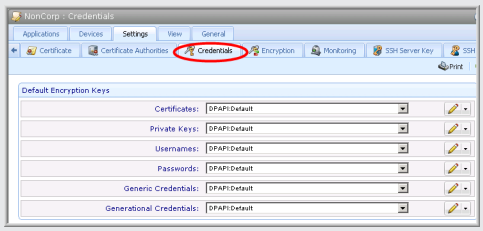
In the Policy tree, folder are used manage which encryption keys are used to encrypt which types of encryption assets.

1. From the Platform menu bar, click Policy Tree.

   You must have the *View* and *Write* permissions to the Policy object to define Policy's default encryption keys.

2. In the Policy tree, select the Policy object where you want to configure object encryption keys.
3. In the Policy object configuration, go to the object configuration tab for the type of object you want to encrypt.

The following table identifies where you can configure the encryption key for each type of encryption asset:

To Encrypt:	Go To:
Certificate Private Keys	Policy > Settings > Certificate tab 
Credential Objects	Policy > Settings > Credentials tab The Credentials tab allows you to assign an encryption key to each type of Credential object: Certificate, Private Key, Username, Password, Generic, and Generational. For more information on Credential objects, see "Working with system credentials" on page 909. 

4. (Optional) Click the  icon to lock the Encryption Key values.

   When you lock an Encryption Key value, Trust Protection Platform uses only the selected encryption key to secure all subordinate objects of that type.

5. Click **Apply**/**Save**.

Viewing the Encryption Keys Used to Secure a Policy's Subordinate Objects

You can view the encryption keys used to secure a Policy's subordinate objects from the Policy object's Encryption tab.

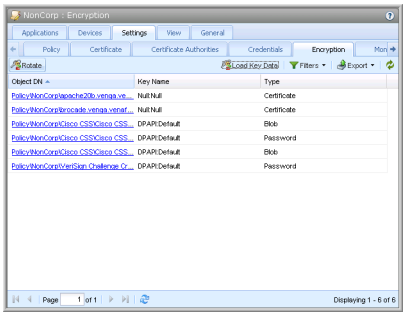
To view the encryption keys used to secure a policy's subordinate objects

1. From the Platform menu bar, click Policy Tree.

   You must have the *View* and *Write* permissions to the Policy object to define Policy's default encryption keys.

2. In the Policy tree, select the Policy object where you want to view object encryption keys.
3. In the Policy object configuration, go to the **Settings > Encryption** tab.
4. Click **Load Key Data**.

   Trust Protection Platform displays the policy's subordinate certificates, SSH keys, and credentials and their associated encryption keys.



Managing encryption keys in the Credentials Tree

In the Credentials tree, the Root Credential object allows you to define the default encryption keys used to secure the Credential objects located in the Credentials tree.

IMPORTANT The Default Encryption Key settings in the Root Credential object apply only to objects in the Credentials tree. To define default values for objects in the Policy tree, you must define the Default Encryption Key settings in folder. For more information, see "Managing encryption keys in the Policy tree" on page 575.

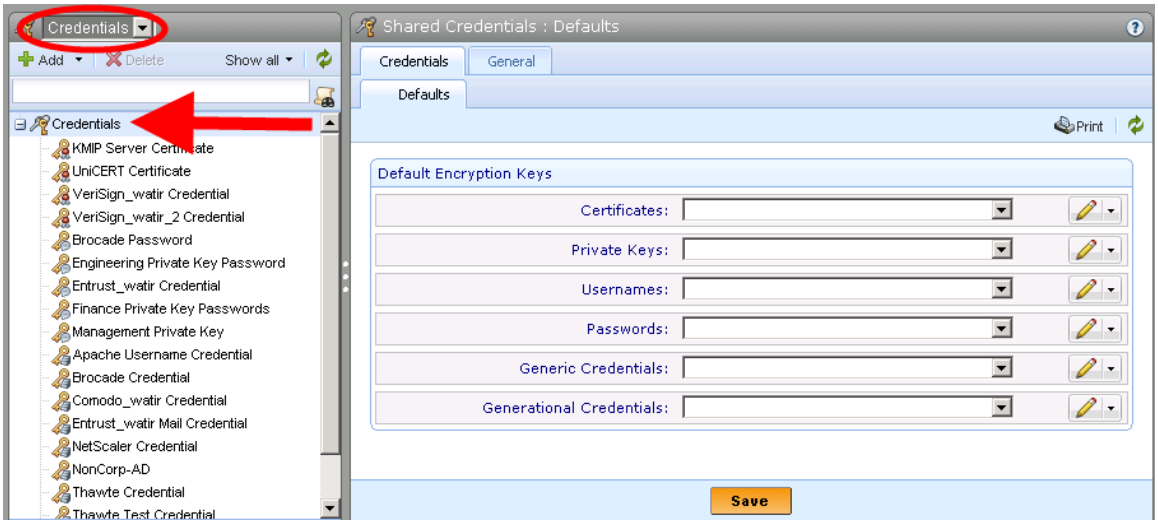
To select your default encryption keys in the Credentials tree

1. From the Platform menu bar, click Policy Tree.

   You must have the View and Write permissions to the Root Credential object to define the default encryption keys.

2. Select the Credentials tree from the Tree drop-down menu.
3. In the Credentials tree, select the Root Credential object.
4. Select the Encryption Key you want to use to encrypt each type of Credential object.

   For more information on Credential objects, see "Working with system credentials" on page 909.



5. (Optional) Click the icon to lock the Encryption Key values.

   When you lock an Encryption Key value, Trust Protection Platform uses only the selected encryption key to secure all subordinate objects of that type.

6. Click **Apply/Save**.

Rotating encryption keys for a policy or ObjectDN

Trust Protection Platform maintains all system information–that is, configuration settings, managed server and certificate information, credentials, SSH server and private keys, and archived certificates–in a database. To secure this information, Trust Protection Platform uses either a software encryption key, a hardware encryption key in a supported HSM, or both to encrypt sensitive information used to connect to the database. Organizations that must periodically rotate their encryption keys can easily do so. After the migration, administrators can verify that all secrets have been re-encrypted with the new encryption key.

Encryption key migration can be handled globally via the Root Encryption Driver object, or it can be handled at the Policy level for the Policy's subordinate objects.

Global key rotation is done in the Venafi Configuration Console. For more information on how to rotate all encryption objects in Trust Protection Platform, see "Rotate Secret Store encryption keys" on page 83 in the *Venafi Administration Guide*.

To rotate encryption keys for a specific Policy object

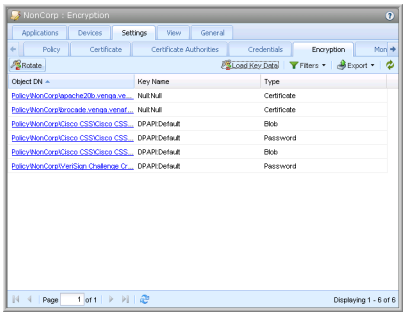
1. From the Platform menu bar, click Policy Tree.

   IMPORTANT You must have master administrator permissions to the root Encryption Driver object. Administrators with Delete permissions to a specific encryption key can also rotate encryption away from that key.

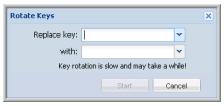
   NOTE This option is provided so that administrators can rotate encryption away from an encryption key before they delete the associated Encryption key object.

2. In the Policy tree, select the Policy object whose encryption keys you want to rotate.
3. Select the **Settings** > **Encryption** tab.
4. Click  **Load Key Data** to display all subordinate objects currently encrypted with an encryption key.

   The **Encryption** tab lists all subordinate objects with an Encryption attribute, even those objects whose encryption is currently set to Null (no encryption).

5. Click  **Rotate**.

6. In the **Replace key** field, designate which encryption key you want to replace.

Encryption is rotated away from this key. All of the policy's subordinate objects currently encrypted with this key will be re-encrypted with the new key.

7. In the **With** field, designate the new encryption key you want to use.

   Encryption is rotated to this key. All of the policy's subordinate objects currently encrypted with the designated replace key will be re-encrypted with this key.

8. Click **Start** to rotate the encryption keys.

   All of the policy's subordinate objects currently encrypted with the designated **Replace key** are re-encrypted with the new key. This includes certificates, private keys, SSH keys, symmetric keys, and all credentials.

NOTE By default, public information such as certificates and public keys are not encrypted. If you rotate the Null key, Trust Protection Platform re-encrypts all objects—even public information—with the new key. Encrypting public information may add unnecessary processing overhead and, depending on the number of objects in your tree and whether your encryption keys are stored on an HSM device, may impact system performance. If you want to rotate encryption for public information such as certificates and public keys back to a Null value, please contact Venafi Support.

Venafi Advanced Key Protect

Venafi Advanced Key Protect is an optional add-on feature to Venafi Trust Protection Platform that allows you to use an HSM for central private key generation, remote key generation, and code signing certificate private key storage.

Before enabling Venafi Advanced Key Protect, contact your Venafi sales representative to understand how this feature will affect your billing.

Venafi Advanced Key Protect is enabled in the Venafi Configuration Console. For more information see "Enabling Venafi Advanced Key Protect" on page 590.

Central private key generation

With central private key generation, Trust Protection Platform generates and stores the private key that is used for the CSR (certificate signing request).

For more information on central private key generation, see "Hardware central key generation with Venafi Advanced Key Protect" on page 585.

Remote private key generation

Remote private key generation means that you are using a supported driver to connect to an HSM where the private key is stored. In this case, Trust Protection Platform never sees the private key. Remote private key generation using an HSM is supported on the following drivers:

- Apache
- CAPI
- JKS

For more information about remote private key generation, see "Hardware remote key generation with Venafi Advanced Key Protect" on page 588.

For more details on the differences between remote private key generation and central private key generation, see "Supported methods of key generation" below.

Supported methods of key generation

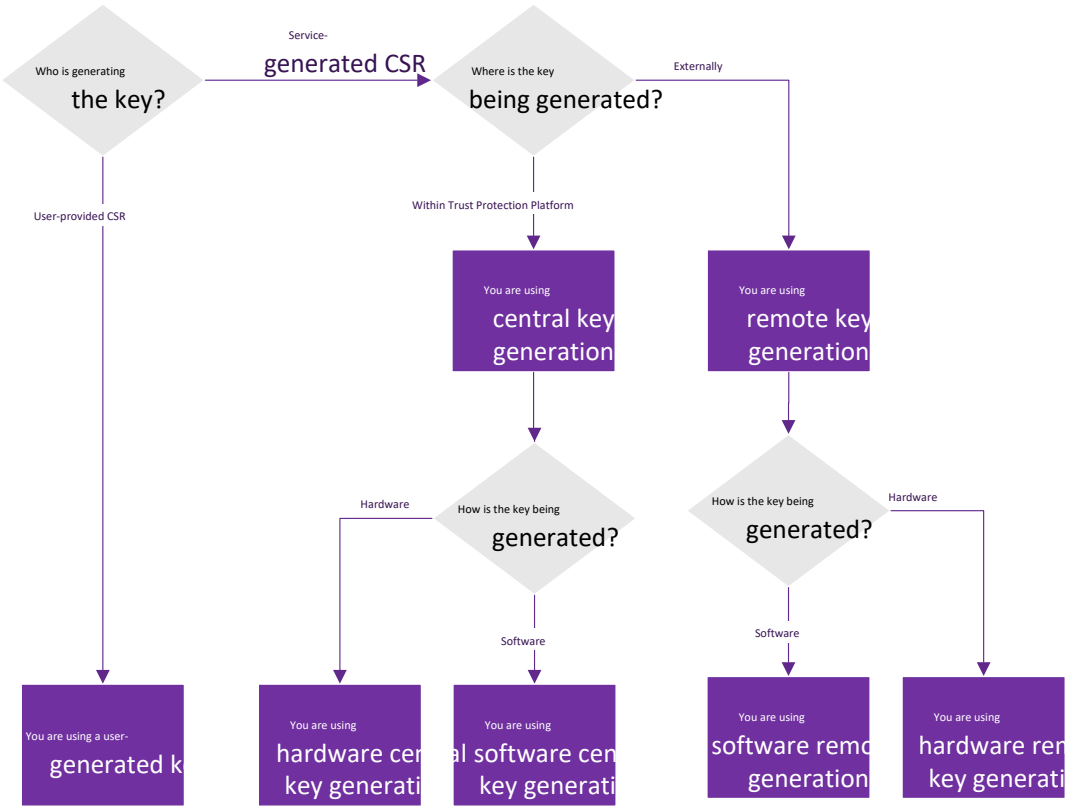
There are a number of ways that keys can be generated for signing CSRs, both in terms of where they are generated (externally or within Trust Protection Platform), and how they are generated (using software or hardware methods).

You can choose whether to generate a private key on Trust Protection Platform, in a remote system, or on an HSM.

IMPORTANT If a certificate is associated with multiple applications, the CSR will always be centrally generated because Trust Protection Platform needs the private key so it can be pushed to all applications. Remote generation is supported only for a 1-to-1 (private key/application) relationship.

Depending on which key generation type you choose, the certificate's private key is stored either in Trust Protection Platform or in the remote system, and the CSR is either generated by Trust Protection Platform or the remote system.

The following chart shows how you can tell which type of key generation you're using, based on who is generating the key, where it is being generated, and how it is being generated.



The following table lists the various types of key generation and gives additional information about each key generation type.

Type	Description	Key Generation Location	Private Key Storage Location	Requires AKP[1]?
User-generated key	When you create the CSR yourself, the key is not stored in Trust Protection Platform, but it might potentially be stored in the system you used to generate the key.	Third-party tool	*not stored*	No
Hardware central key generation	With hardware central key generation, Trust Protection Platform connects directly to the HSM and instructs the HSM to create the private key. Trust Protection Platform then exports the key from where it is stored. Trust Protection Platform uses the key to sign the CSR.	HSM	Trust Protection Platform (For code signing, can either be in Trust Protection Platform or the HSM)	Yes

[1]Venafi Advanced Key Protect

Type	Description	Key Generation Location	Private Key Storage Location	Requires AKP[1]?
Software central key generation	With software central key generation, Trust Protection Platform generates and stores the private key. It then uses the key to sign the CSR.	Trust Protection Platform	Trust Protection Platform	No
Hardware remote key generation	With hardware remote key generation, Trust Protection Platform connects to the remote HSM, and instructs the remote system (via a supported driver) to generate the private key using hardware generation. It then stores the private key on the HSM, and then creates the signed CSR, which is then exported to Trust Protection Platform. In this case, Trust Protection Platform never sees the private key, just the signed CSR. The key remains in the HSM.	HSM connected to remote system	HSM connected to remote system	Yes
Software remote key generation	With software remote key generation, Trust Protection Platform connects to the remote system, and instructs the remote system to use software to generate a private key. It then stores the private key on the remote system, and creates the signed CSR, which is then exported to Trust Protection Platform. In this case, Trust Protection Platform never sees the private key, just the signed CSR. The key remains on the remote system.	Remote system	Remote system	No

[1]Venafi Advanced Key Protect

To learn about the lifecycle stages of a Trust Protection Platform certificate, see About certificate lifecycle management.

Stages	Remote key generation storage	Central key generation storage
0-400	Remote system (called **Application** in Policy Tree)	Trust Protection Platform
500-700	Certificate Authority	Certificate Authority
800-1200	Remote system (called **Application** in Policy Tree)	Application

Hardware central key generation with Venafi Advanced Key Protect

With hardware central key generation, Trust Protection Platform connects directly to the HSM, and instructs the HSM to create the private key. Trust Protection Platform then exports the key where it is stored. Trust Protection Platform uses the key to sign the CSR.

Using an HSM for private key generation for SSH keys and certificates

Once Venafi Advanced Key Protect is enabled on your system, if you want to use an HSM to generate private keys for certificates, you can either configure the Key Generation option at the policy level (on the Certificate tab) in Policy Tree, or you can change the Default Key Generation option on the encryption tree root.

If you want to use the HSM for generating SSH keys and a software driver for certificates, you need to set the Default Key Generation option on the encryption tree root to the HSM in Policy Tree. For certificates, you can override this setting by changing the Key Generation option on the Certificate tab at the policy level. For configuration information, see "Configuring the root encryption driver" on page 549.

Venafi Advanced Key Protect system requirements for supported HSMs

Starting with the specified client versions, the following HSMs are supported for central key generation by Venafi Advanced Key Protect and private key storage for Venafi CodeSign Protect.

IMPORTANT Venafi recommends you consult the partner documentation for minimum supported versions.

TIP The following tables show vendor support for generating private keys. In all cases, this refers to Hardware Central Key Generation. Learn more about "Supported methods of key generation" on page 581.

Supported HSM	Docs	Encrypt Secrets	HCKG for private keys[1]	Code Signing Certificate Private Key Storage[2]
Entrust nShield Connect HSM	Partner PDF	✔	✔	✔
Thales SafeNet Luna SA (including Azure Dedicated HSM)	Partner Docs	✔	✔	✔

Vendor Self-Certified HSMs

NOTE The HSM Partners on the list below have gone through the process of self-certification. This process involves testing the specific PKCS#11 mechanisms that Trust Protection Platform uses when an HSM is used to protect things like private keys and credential objects, and when Advanced Key Protect is enabled.

Self- certification means that the partner has done the testing and proven successful results and integration with Venafi. Successful self-certification results indicate that the integration will work as expected. The HSM vendor may need to be engaged if something is working unexpectedly. Consult the partner's documentation to know what firmware version requirement is.

HSM Vendor *HSM Product*	Docs	Encrypt Secrets	HCKG for private keys[3]	Code Signing Certificate Private Key Storage[4]
Atos *Trustway Proteccio*	PDF (no public link; contact vendor)	✔	✔	✔
AWS CloudHSM	Venafi Docs	✔		✔
Crypto4A		✔	✔	✔

[1]Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.
[2]Requires **Venafi Advanced Key Protect** add-on module
[3]Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.
[4]Requires **Venafi Advanced Key Protect** add-on module

HSM Vendor *HSM Product*	Docs	Encrypt Secrets	HCKG for private keys[1]	Code Signing Certificate Private Key Storage[2]
QxEDGE				
Entrust *Entrust nShield as a Service*	Partner Docs	✔	✔	✔
Fortanix *Fortanix DSM*	Partner Docs	✔	✔	✔
FutureX *Vectra Plus*	Partner Docs	✔	✔	✔
Gradiant *KeyConnect*				✔
Securosys *Primus HSM* and *Cloud HSM Service*	Partner Docs (Login required)	✔	✔	✔
Thales TCT *T-Series Luna*	Partner Docs	✔	✔	✔
Thales *Data Protection on Demand*	Partner Docs	✔	✔	✔
Utimaco *CryptoServer*	Partner Docs (Login required)	✔	✔	✔

[1]Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.

[2]Requires **Venafi Advanced Key Protect** add-on module

Hardware remote key generation with Venafi Advanced Key Protect

With hardware remote key generation, Trust Protection Platform connects to the remote HSM, and instructs the remote system (via a supported driver) to generate the private key using hardware generation. It then stores the private key on the HSM, and creates the signed CSR, which is then exported to Trust Protection Platform. In this case, Trust Protection Platform never sees the private key, just the signed CSR. The key remains in the HSM.

The supported drivers are:

- Apache. For more information on configuring Apache certificates, see "Enabling remote key generation for Apache certificates" on page 590.
- CAPI. For more information on configuring CAPI certificates, see "Enabling remote key generation for CAPI certificates" on page 593.
- JKS For more information on configuring JKS certificates, see "Enabling remote key generation for JKS certificates" on page 594.
- F5 LTM Advanced For more information on configuring F5 certificates, see Configuring an F5 LTM Advanced application object.

Hardware remote key generation is the most secure method of generating private keys and CSRs because the data stays remotely in the HSM.

Managing applications using HSM-protected keys and Venafi Advanced Key Protect

Hardware security modules (HSMs) offer a way to provide a higher level of security by generating private keys within a protected domain from which they're never permitted to leave. This means that an attacker would have to do all traffic decryption work from the application server they compromised, which would then put themselves at much greater risk of being detected.

Interfacing an application server with an HSM requires additional software, configuration, and expense.

HSMs are generally reserved for protecting the most mission-critical applications and those that manage highly sensitive data. Venafi can automatically process generating keys inside Thales SafeNet Luna SA and Entrust nShield HSMs using the following provisioning drivers:

- Apache
- CAPI
- JKS

Using remote key generation via an application driver to an HSM allows the HSM to complete the full certificate lifecycle. This remote generation requires that target devices have the necessary HSM client software installed and properly configured.

EXAMPLE The following diagram provides an overview of how you configure your HSM using Trust Protection Platform, an application server (running Apache, Java, or IIS), your HSM client utility and HSM server, and your CA.

1. Execute command to generate keypair inside the HSM by Trust Protection Platform using your HSM's client utilities and is remotely executed from the Apache/Java/IIS host (the Application server).
2. Execute command to generate CSR on the application server (Apache/Java/IIS host) using your HSM's client utilities and then executed, retrieved, and submitted by Trust Protection Platform to the CA.
3. A certificate is issued by the CA and then retrieved and provisioned by Trust Protection Platform to the application server (Apache/Java/IIS host).

IMPORTANT If you want to configure remote key generation using an HSM, you must activate Venafi Advanced Key Protect, an optional add-on feature to Venafi Trust Protection Platform. For more information, see "Venafi Advanced Key Protect" on page 580 in the *Trust Protection Platform Administration Guide*.

Normally remote generation only supports one certificate to one application. If you want to install a certificate to many locations, the HSM can do central generation. However, if you are an Advanced Key Protect customer and have HSM connected Apache installations, we do support installing a single certificate to many Apache servers and making sure the Apache is configured to access the private key on the HSM properly. For special configuration information, see Configuring HSM-based remote key generation.

DID YOU KNOW? In asymmetric encryption, security relies upon private keys remaining private. Limiting access to private keys is essential to ensuring that network communications between client and server are secure and protected. This is typically done by setting permissions on keystore files at the operating system level of the computer hosting the certificate and by applying password-based encryption on the keystore itself.

Although this method protects the private key from unauthorized access, it does not prevent a privileged user (or an attacker who has stolen a privileged user's credentials) from exfiltrating the keystore from the computer and using readily available password-cracking methods to obtain the private key. The possessor of a stolen private key can decrypt communications between the client and server putting sensitive data at risk.

Enabling Venafi Advanced Key Protect

With Venafi Advanced Key Protect, you can use an HSM to generate keys and, in the case of CodeSign Protect, store private keys remotely. This is an optional add-on feature to Venafi Trust Protection Platform.

To enable or disable Advanced Key Protect

1. On the Venafi Trust Protection Platform server, open the Venafi Configuration Console, and click the Connectors node.
2. In the Actions panel, click **Enable Advanced Key Protect** (or **Disable Advanced Key Protect**).
3. Review the information in the dialog boxes and confirm the action.
4. Restart the IIS service by going to the **Product** node, and clicking on **Website**, and then clicking **Restart**.
5. Restart the Venafi Platform service by clicking on **Venafi Platform**, and then clicking **Restart**.
6. Restart the Logging service by clicking on **Logging**, and then clicking **Restart**.

The change is reflected on the License Report that is automatically submitted to Venafi. For information about the license report, see Venafi License Report.

Enabling remote key generation for Apache certificates

After you enable Venafi Advanced Key Protect enabled, you enable specific installations to use remote key generation. For example, if you want Thales SafeNet Luna SA HSM-based remote key generation to share a certificate across several HTTP Apache servers, you enable each Apache installation.

Configuring remote key generation for Apache

1. In TLS Protect, locate a certificate with installations of type Apache.
   a. Open the **Certificate Inventory**.
   b. Use the **Installation Type** filter to limit installations to Apache.
2. In the **Installations** column, click the arrow to see the installations associated with a certificate.
3. In the **Installation Type** column, look for installations of type Apache, and then click **Installation Type**.
4. Click **Edit**.
5. Scroll to the **Hardware Security Module Settings** section.

   These settings are only available if you have Venafi Advanced Key Protect enabled. For more information, see "Enabling Venafi Advanced Key Protect" on the previous page.
6. In the **Private Key Location** field, choose hardware remote key generation or software remote key generation. For more information, see "Supported methods of key generation" on page 581.
   - **Device**. This option is software remote key generation on the external device.
   - **Thales SafeNet HSM**. This option is hardware remote key generation on the Thales SafeNet Luna SA HSM. You will be required to fill out the following fields:
     - **Client Tools Path**. Type the directory path where the `sautil` command from the OpenSSL Toolkit is located on the device.

       The default path is `/usr/safenet/lunaclient/bin`.
     - **Partition Password Credential**. Select a password credential that represents the PIN for the HSM partition where the private key is stored.

       If the credential doesn't yet exist, click **Create New Credential**.
   - **Entrust nShield Connect HSM** (RSA keys only). This option is hardware remote key generation on the Entrust nShield Entrust nShield Connect HSM. If you choose Entrust nShield Connect HSM, you must fill out the following fields:
     - (Conditional) **Common Data Location**. Type the directory path where the HSM will store the certificate and private key. The default is */opt/nfast/kmdata/local*.

> **DID YOU KNOW?** The **Common Data Location** is the directory where Trust Protection Platform fetches additional Entrust nShield Connect HSM artifacts. If you are using Entrust nShield Connect HSM-based remote key generation in a group, be sure to specify a valid path for **Common Data Location**. Otherwise, during Stage 801, a '"no such file" error occurs. The default is */opt/nfast/kmdata/local*.

- **Client Tools Path**. Type the directory path where the `generatekey` utility and other nShield Core Tools are installed on the device.

  The default path is `/opt/nfast/bin`.

- **Protection Type**. Depending on the option you select, you might also have to specify an **Identifier** for the protection type selected.

  - **Operator Card Set.** Enter the OCS Identifier.

    > **IMPORTANT** Only operator card sets with a quorum of 1 are supported (1-of-N) and the operator card must be inserted into the HSM's card reader slot prior to any interaction by Trust Protection Platform with the device. *An operator card may be left permanently inserted into the slot; or you can configure a workflow to pause processing until someone has acknowledged reinsertion of the card.*

  - **Module**. This is the lowest protection level. It requires that your device has been properly configured to use the HSM for key generation.

  - **Softcard**. This is the next highest level of protection. This is a kind of password that is stored on your HSM. If you selected Softcard as the Protection Type, then in the **Softcard Identifier field**, enter your softcard's 40-character hash.

    This option requires that the device is properly configured to use the HSM for key generation and that a softcard has been previously generated using the HSM, and that the requester knows the passphrase for that softcard.

    > **NOTE** If you set **Reuse Private Key for Service Generated CSRs** to *Yes* on a certificate's policy, the protection type is ignored because it cannot be changed for an existing private key. If you need to change the protection type, you must set **Reuse Private Key for Service Generated CSRs** to No.
    >
    > For more information, see Setting policy on a folder (Aperture).

- **Softcard Identifier**. Type the 40-character hash that identifies the soft card.

- **Softcard Password Credential**. Type a password credential that provides the softcard pass phrase.
- **Private Key Alias**. Displays the HSM key alias value for this key using the Private Key Label Apache object attribute (to save the data).

  While this read-only field is visible on every Apache application object, it is only enabled for Entrust nShield's Entrust nShield Connect HSM option.

  The private key alias is created by combining the time-stamp (`YYMMDDhhmmss`) and file name of the key (without the file extension). Example, `190316142039_MyPrivateKey`.

7. Click **Save**.
8. (Optional) If you are using a SafeNet HSM that runs in strict FIPS 140-2 Level 3 mode, configure it with `RSAKeyGenMechRemap=1`. For more information, see SafeNet documentation.

TIP You can control the remote generation settings via policy by launching Policy Tree, selecting a policy, and opening **Applications** > **Apache** > **Remote Generation Settings**.

Enabling remote key generation for CAPI certificates

If you have Venafi Advanced Key Protect enabled, you can enable specific installations to use remote key generation.

Configuring remote key generation for CAPI

1. In TLS Protect, locate a certificate with installations of type CAPI.
   a. Open the **Certificate Inventory**.
   b. Use the **Installation Type** filter to limit installations to CAPI.
2. In the **Installations** column, click the arrow to see the installations associated with a certificate.
3. In the **Installation Type** column, look for installations of type CAPI, and then click **Installation Type**.
4. Click **Edit**.
5. Scroll to the **Hardware Security Module Settings** section.

   These settings are only available if you have Venafi Advanced Key Protect enabled. For more information, see "Enabling Venafi Advanced Key Protect" on page 590.

6. In the **Private Key Location** field, choose hardware remote key generation or software remote key generation. For more information, see "Supported methods of key generation" on page 581.
    - **Device**. This option is software remote key generation on the external device.
    - **Thales SafeNet HSM**. This option is hardware remote key generation on the Thales SafeNet Luna SA HSM. You will be required to fill out the following fields:
        - **Key Label.** Type the label that you want used for keys created by the CAPI driver in your HSM.

          This option makes it easier for you to identify which certificates correspond to the newly generated keys. If you leave this field empty, Windows automatically generates a unique name whenever a new key pair is created. Alternatively, you could choose to change the key label manually before renewing the certificate.

          > **DID YOU KNOW?** Trust Protection Platform uses the label you specify each time that it provisions the certificate. Because Microsoft Windows allows only one instance of a particular key label, you must set Reuse Private Key for Service Generated CSRs to Yes on the certificate's policy, which prevents a possible error the first time the certificate is renewed. For more information, see Policy object certificate settings and Setting policy on a folder (Aperture).
    - **Entrust nShield Connect HSM** (RSA keys only). This option is hardware remote key generation on the Entrust nShield Entrust nShield Connect HSM. If you choose Entrust nShield Connect HSM, no additional configuration information is required.
7. Click **Save**.
8. (Optional) If you are using a SafeNet HSM that runs in strict FIPS 140-2 Level 3 mode, configure it with `RSAKeyGenMechRemap=1`. For more information, see SafeNet documentation.

> **TIP** You can control the remote generation settings via policy by launching Policy Tree, selecting a policy, and opening **Applications** > **CAPI** > **Remote Generation Settings**.

Enabling remote key generation for JKS certificates

If you have Venafi Advanced Key Protect enabled, you can enable specific installations to use remote key generation.

Configuring remote key generation for JKS

1. In TLS Protect, locate a certificate with installations of type JKS.
   a. Open the **Certificate Inventory**.
   b. Use the **Installation Type** filter to limit installations to JKS.
2. In the **Installations** column, click the arrow to see the installations associated with a certificate.
3. In the **Installation Type** column, look for installations of type JKS, and then click **Installation Type**.
4. Click **Edit**.
5. Scroll to the **Hardware Security Module Settings** section.

   These settings are only available if you have Venafi Advanced Key Protect enabled. For more information, see "Enabling Venafi Advanced Key Protect" on page 590.
6. In the **Private Key Location** field, choose hardware remote key generation or software remote key generation. For more information, see "Supported methods of key generation" on page 581.
   - **Device**. This option is software remote key generation on the external device.
   - **Thales SafeNet HSM**. This option is hardware remote key generation on the Thales SafeNet Luna SA HSM. You will be required to fill out the following fields:
     - **Slot Number.** Type the HSM slot number used by your JKS.
   - **Entrust nShield Connect HSM** (RSA keys only). This option is hardware remote key generation on the Entrust nShield Entrust nShield Connect HSM. If you choose Entrust nShield Connect HSM, you must fill out the following fields:
     - **Java Vendor.** Select the vendor of the JDK you have installed on the device (either Oracle or IBM)
     - **Protection Type**. Depending on the option you select, you might also have to specify an **Identifier** for the protection type selected.
       - **Module**. This is the lowest protection level. It requires that your device has been properly configured to use the HSM for key generation.

- **Softcard**. This is the next highest level of protection. This is a kind of password that is stored on your HSM. If you selected Softcard as the Protection Type, then in the **Softcard Identifier field**, enter your softcard's 40-character hash.

  This option requires that the device is properly configured to use the HSM for key generation and that a softcard has been previously generated using the HSM, and that the requester knows the passphrase for that softcard.

  > **NOTE** If you set **Reuse Private Key for Service Generated CSRs** to *Yes* on a certificate's policy, the protection type is ignored because it cannot be changed for an existing private key. If you need to change the protection type, you must set **Reuse Private Key for Service Generated CSRs** to No.
  >
  > For more information, see Setting policy on a folder (Aperture).

7. Click **Save**.
8. (Optional) If you are using a SafeNet HSM that runs in strict FIPS 140-2 Level 3 mode, configure it with `RSAKeyGenMechRemap=1`. For more information, see SafeNet documentation.

> **TIP** You can control the remote generation settings via policy by launching Policy Tree, selecting a policy, and opening **Applications** > **JKS** > **Remote Generation Settings**.

10

Using the dashboards

The Venafi Trust Protection Platform™ dashboards are the default view when you open the web console. The various dashboards offer a high-level snapshot of the state of your security environment, giving you at-a-glance insight about potential areas of concern. Remember, however, you can view only information for objects to which your account has been given permissions.

There are four dashboards in the system, and depend on which product you are using:

- **All Certificates (dashboard)**: Gives insight into the certificates in your network that you have permission to view. Availability of this dashboard is determined by your Trust Protection Platform license.

  Primary dashboard for TLS Protect.

  Also available in SSH Protect, Client Protect, and Platform products.

  For more information, see "Working with the All Certificates (dashboard)" on page 599.

- **SSH Keys (dashboard)**: Shows information about SSH keys in your network that you have permission to view. Availability of this dashboard is determined by your Trust Protection Platform license.

  Primary dashboard for SSH Protect.

  Also available in TLS Protect, Client Protect and Platform products.

For more information, see "Working with the SSH Keys (dashboard)" on page 618.

- **User and Client Device Certificate (dashboard)**: Similar to the All Certificates (dashboard), but shows only the user and client device certificates. Availability determined by your Trust Protection Platform license.

  Primary dashboard for Client Protect.

  Also available in TLS Protect, SSH Protect,and Platform products.

  For more information, see "Working with the User and Client Device Certificate (dashboard)" on page 610.

- **System Status (dashboard)**: Shows information about the Trust Protection Platform servers, or engines, that are connected to the underlying Trust Protection Platform database. This dashboard is available for all licensed products, but visibility is determined by role. By default, only users with the *Master Admin* role can see this dashboard. To grant others visibility to this dashboard, give them *read/write* permissions to the root folder of the Platform tree in Policy Tree.

  Individual widgets represent distinct Trust Protection Platform servers.

  Primary dashboard for Platform.

  Also available in TLS Protect, SSH Protect, and Client Protect products.

  For more information, see "Working with the System Status (dashboard)" on page 629

- CodeSign Protect (dashboard): Gives a high-level view of the number of projects, environments, users, and signings are happening in the CodeSign Protect product.

  Available in CodeSign Protect.

This chapter contains the following topics:

About Dashboard widgets 599

Working with the All Certificates (dashboard) 599

Working with the User and Client Device Certificate (dashboard) 610

Working with the SSH Keys (dashboard) 618

Working with the System Status (dashboard) 629

Configuring value thresholds using Account Preferences 631

About Dashboard widgets

Dashboards are customizable. You can add or remove widgets that provide valuable details. You can click a widget's graph to open the List View to see more information about the data presented in the widget.

The power of dashboard widgets is their ability to not only highlight trends and potential risks, but also to provide one-click access to details and actions you can take to remedy those risks, which is a critical component of a strong security strategy.

To add a widget to a dashboard

- Click the **Add Widget** button in the top right corner of the Dashboard page, then select the widget you want to add.

To remove a widget from a dashboard

- Hover over the top right corner of the widget until you see ✕, and then click ✕.

To move a widget to a new location on a dashboard

- Hover the pointer over the widget until the pointer becomes  , then drag the widget to a new location on the screen.

Some widgets can be configured to show specific data. If a widget can be edited, when you hover the mouse pointer over a widget, you see . Click to see what configurations you can make.

> **NOTE** Widgets require some historical data in order to provide value. For example, the Trends widget cannot provide trending data about private key orphans until orphans have been found and tracked for at least a few days.

Working with the All Certificates (dashboard)

The All Certificates (dashboard) gives you insight into the various certificates in your system that you have access to see. The widgets on the All Certificates (dashboard) are listed on the right side of this page.

Certificate Authorities widget

This widget displays the number of certificates by the issuing certificate authority (CA), including self-signed certificates. This can help ensure that you are using CAs according to your own trust policies.

Certificate Expiration widget

Expired certificates create a serious threat. The Certificate Expiration widget helps you stay ahead of the risk curve by showing certificates that have upcoming expiration dates. You can customize the date range shown in the widget by clicking the date range drop-down box near the widget title. On the graph, you can hover over a bar to see the validity period for that bar and the number of certificates represented by that bar. Clicking the bar opens the Certificate Inventory filtered to just those certificates.

What do the colors mean?

The Certificate Expiration widget utilizes specific colors to make it easy to identify the state of each certificate.

Blue: Certificates that are in an expired state.

Red: A critical state showing certificates that either have already expired, or that will expire within the next 15 days or less.

Yellow: Indicates a less critical state showing certificates that will expire within the next 16 to 30 days.

Green: These certificates are considered secure because their expiration dates are out 30 days or further.

- To view details and to take action, click a bar.

Certificate Key Size widget

Certificates contain cryptographic keys that are used to protect information and/or authenticate users or devices.

The length of a cryptographic key determines how difficult it is to break. The U.S. National Institute of Standards and Technology (NIST) recommends that all organizations stop using keys that are less than 2048-bits for asymmetric algorithms (e.g., RSA, DSA, Diffie-Hellman) by the end of 2013.

Using the Certificate Key Length widget, you can easily identify keys in your environment that are smaller than 2048.

BEST PRACTICE To better secure and protect your environment, replace all certificates in which the key length is below 2048.

NOTE A key length of zero (0) indicates an ECC (Elliptic-curve cryptography) certificate.

Certificate Protection Level widget

The Certificate Protection Level widget identifies certificates by management type. The management types are:

- **Unassigned**. These certificates are neither enrolled or monitored by Trust Protection Platform.
- **Monitoring**. These certificates are continuously monitored for expiration and associated risks.
- **Enrollment**. At this level, Trust Protection Platform interfaces directly with Certificate Authorities (CAs) to initiate and auto-enroll new or to-be-renewed certificates and key generation requests according to organization-defined workflow and approved policies.
- **Certificate Installation (Provisioning)**. These certificates are enrolled and automatically provisioned by Trust Protection Platform to web servers and appliances that use them.

For more information about these protection levels, see Certificate Management.

Certificate Signing Algorithm Widget

Certificates are digitally signed by certificate authorities (CAs) to ensure their authenticity. Digital signatures are applied using message digest or hash algorithms (such as MD5 and SHA1) and asymmetric algorithms (such as RSA and DSA). They are typically named using a combination of each algorithm type, such as MD5RSA or SHA1RSA.

The National Institute of Standards (NIST) and other standards organizations provide guidance on algorithms that are considered secure. Use the Certificate Signing Algorithm widget to help ensure that your certificates are in compliance with their recommendations.

Certificate Totals widget

The Certificate Totals widget gives you an overview of important certificate data and provides a quick way for you to access filtered lists of certificates in your inventory. This widget is comprised of pre-defined tiles that you can enable or disable as needed. Some of the tiles can be customized to fit your needs. Clicking the number in any tile opens a filtered list in the certificate inventory where you can view the certificates in detail.

Available tiles

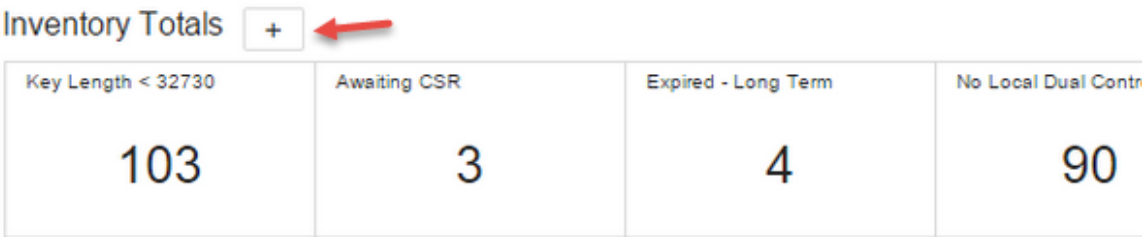
- **Awaiting CSR.** Number of certificates waiting to be approved by a CA.
- **Distrusted Entrust.** Number of certificates issued by one of the following CAs:
  - Entrust
  - AffirmTrust

  Some web browsers flag these certificates as a potential security risk.
- **Expired < 30 days**. Number of certificates that expired less than 30 days ago. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 604.
- **Expired > 30 days**. Number of certificates that expired more than 30 days ago. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 604.
- **Expiring within 30 days**. Number of certificates that expire in the next 30 days. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 604.
- **Failed Revocation.**
- **Failed Validation.**
- **In Error.**
- **Key Size < 1024.** Number of certificates that have a key size less than 1024 bits. The key size threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 604.
- **Local Dual Control Needed.** Number of certificates that might not have a reviewer or approver with local knowledge.

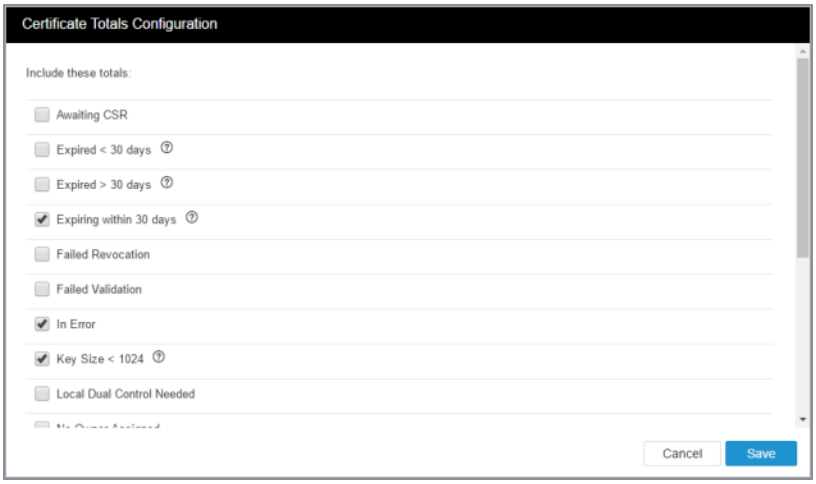
- **No Owner Assigned.** Number of certificates that have no assigned contact.
- **Pending My Approval.** Number of certificates that you need to take action on, because you have been assigned to approve them. These certificates may be in any state.
- **Total Certificates.** Number of certificates that you have permissions to, including Retired and Lost certificates.
- **Total Managed Certificates**. Number of certificates that you have permissions to, excluding Retired and Lost certificates.
- **Total Retired Certificates**.
- **Unapproved Issuer**. Number of certificates that have been issued by a CA that is not approved in Trust Protection Platform. To learn how to approve a certificate issuer, see Approving a certificate issuer (CA).
- **Validity Periods.** Shows the total number of certificates that exceed the default validity period (specified in days). The validity period is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on the next page.
- **Weak Signing Algorithm**: Number of certificates not signed by one of the algorithms defined in Account Preferences. See "Configuring or editing a tile" on the next page.

Adding tiles

1. Click + .



2. In **Widget Configuration**, select the tiles you want to add.



3. Click **Save**.

Removing Tiles

Hover over the tile you want to remove, and click the ✕ in the top right corner of the tile.

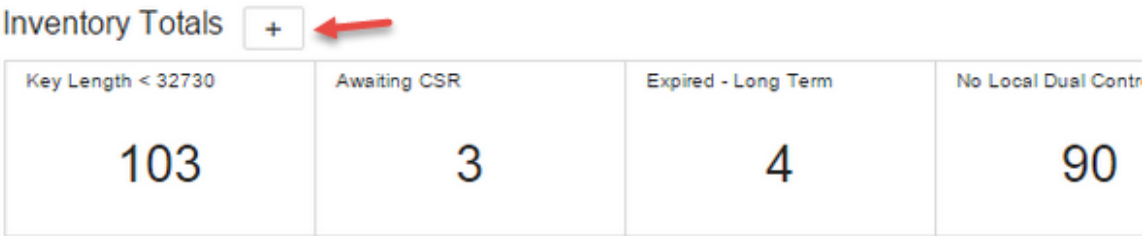
Reordering tiles

Hover the pointer over the tile until the pointer becomes ✥, then drag the widget to a new location.

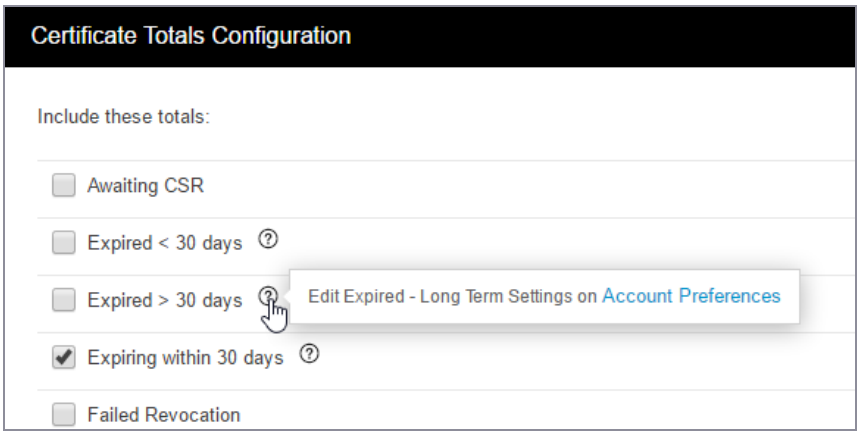
Configuring or editing a tile

A number of the tiles can be customized to show values that meet your specifications.

1. Click **+**.



2. Tiles that can be customized have a help icon ⓘ. If you want to edit the value of a tile, click the help icon, and then click the **Account Preferences** link. For more information, see "Configuring value thresholds using Account Preferences" on page 631.



Certificate Trends widget

The Trends widget provides a burn-down chart view that can help you to easily identify trends within certificate management. Using the drop-down selectors at the top of the widget, you can select what trend you'd like to see and over what period of time you'd like to see it.

> **NOTE** Widgets require some historical data in order to provide value. For example, the Trends widget cannot provide trending data about private key orphans until orphans have been found and tracked for at least a few days.

When the agent checks in with Trust Protection Platform and has changes to report, the graph is updated when any changes have been discovered by the agent.

The Trends widget on the All Certificates (dashboard) lets you track the following key indicators:

Trend	Description
Key Size	Displays the trend for each key length from 512 up to 4096. This trend can help to identify when and to what extent weaker key lengths are being used.
Signing Algorithm	Displays the number of certificates grouped by Digital Signature Algorithms (signing algorithm), which can help you evaluate risk and company security policy compliance.
Key Algorithm	Shows the algorithm used to generate the key. RSA and ECC are the two types of algorithms used.
Management Type	Displays the number of certificates by management type over time. Management types include: ■ **Monitoring** ■ **Enrollment** ■ **Provisioning** ■ **Unassigned**: Unlicensed Trust Protection Platform certificates and keys that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.
Issuer	Displays certificates by their originating CAs, including self-signed certificates.
Validity Period	Displays the number of certificates by validity period, or the amount of time before certificates expire (0 to 1 year, 2 years, and 3 years, respectively).
Certificate Type	Shows the types of certificates: Device User.
Total Certs	Indicates the total number of certificates under Trust Protection Platform management.
Renewal	Shows the number of renewals that are going to happen on each calendar day that is displayed in the widget.
Protection Status Summary	The difference between the graph line showing the total number of certificates and the line showing the total number of secured certificates provides a clear view of how secure your certificate inventory really is.

Certificate Validity Period widget

A certificate's validity period is the length of time that a certificate is valid for use. The longer a certificate is valid, the greater the possibility that the private key used with that certificate has been compromised.

Private keys used with certificates are susceptible to internal and external compromise. For example, in order to manage certificates, many administrators have direct access to private keys and can make copies of them. This represents a significant risk if an administrator is reassigned or terminated and the certificates and private keys they were managing are not replaced for an extended period of time.

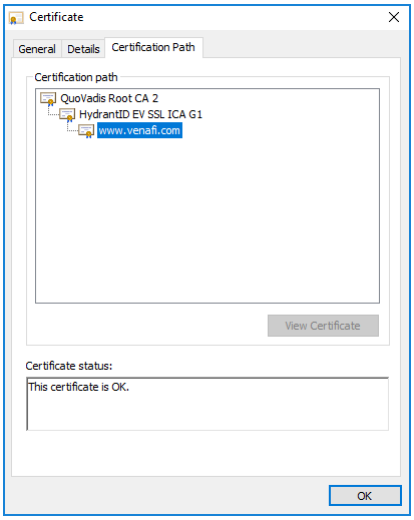
Minimizing certificate validity periods helps ensure that certificates are replaced regularly. To reduce the risk of compromise, certificate validity periods of one year or less should be used.

The Certificate Validity Period widget helps you to easily identify the age of your certificates so that you can adhere to this best practice.

Chain Validation widget

Certificates can be chained, which means that a certificate may be signed by one or more intermediate signing authorities authorized by a CA to issue certificates on their behalf. The chain is from the certificate installed on the web server, to its intermediate authority (or authorities), and finally up to the certificate authority.

For example, the following graphic shows how you can see (in a web browser) the certificate chain for the website (end-entity) back to the root CA.



Trust Protection Platform provides the ability to validate the entire chain for a certificate, helping ensure that all certificates in the chain are valid, and are not at risk for failure. This is critical to monitor, because if any certificate in the chain expires, is revoked, or otherwise becomes invalid, there will be an outage. The Chain Validation widget shows counts of certificates in your system, grouped by chain validation result. Hovering over one of the bubbles in the chart displays the chain validation results and the number of certificates that match those results. (This does not show the number of installations of a certificate.)

The following table lists the types of results you may see in your chain validation widget.

Status	Category
Success	Success (green)
Expiring CA in chain	Outage Risk Failures (red)
Could not build chain	General Failures (orange)
Mismatched chain	General Failures (orange)
Mismatched endpoint certificate	General Failures (orange)
No chain returned	General Failures (orange)
Incomplete chain	General Failures (orange)

Outage Risk Failures (red bubbles) require your immediate attention, as they present the greatest risk of imminent potential outages.

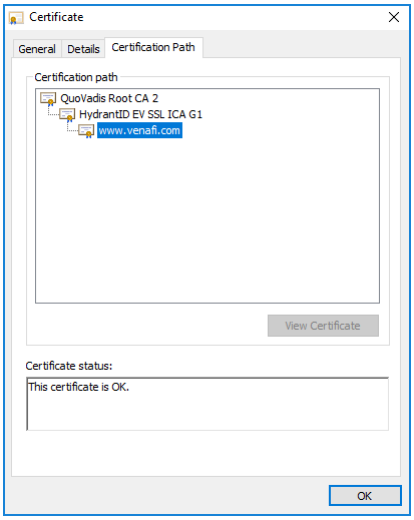
> **NOTE** A certificate may be in more than one bubble at a time, and even in more than one item in the graph's key. For example, if a certificate failed chain validation because there was an outage risk failure, and a mismatched endpoint failure, the certificate would be counted in the key in both the Outage Risk Failures category, as well as the General Failures category in the key.

Click a bubble to see a filtered list of certificates that match that bubble status. You can also click on the description in the key to see a filtered list of certificates that match that validation result. On the filter results page, click the down arrow in the TLS Endpoints column to see specific installation validation information.

End Entity Validation widget

An end entity (also called a leaf) may be a website or server with a certificate (for example, an LDAP server). The end entity is the last certificate in the certificate chain (the leaf certificate that chains up to the root certificate). For example, in the following image, the highlighted certificate is the end-entity for

this certificate.



On the All Certificates (dashboard), the End Entity Validation widget shows certificates that have and have not been able to be validated to their named end entity. Hovering over one of the bubbles in the chart displays the end entity validation results and the number of certificates that match those results. (This does not show the number of validation endpoints.)

> **NOTE** A certificate may be in more than one bubble at a time. For example, if a certificate failed end entity validation because there was a connection failure AND because there was no certificate match, the certificate will show up in both bubbles. However in this example, both failures are grouped under "General Failures" in the graph's key, so it will only be counted one time in the key.

Click a bubble to see a filtered list of certificates that match that bubble status. You can also click on the description in the key to see a filtered list of certificates that match that validation result. On the filter results page, click the down arrow in the TLS Endpoints column to see specific installation validation information.

Secure Protocols vs Insecure Protocols widget

Applications or appliances that are TLS web servers can be configured to support multiple SSL or TLS protocols, so for good security it is important to know which protocols are enabled. Venafi supports the following communication protocols SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Leaving insecure protocol versions enabled can leave you vulnerable to attacks where hackers force connections to your server to use older versions of the protocols that have known exploits. This can leave your encrypted connectors (whether between a site visitor and your web server, or a machine-to-machine connection) open to a man-in-the-middle, or other type of attack. Thus it is important to know if the

certificates used to protect your systems connect via a secure or an insecure protocol. Trust Protection Platform considers anything less than TLS 1.2 as insecure. Connections via an insecure protocol version can present a significant security risk to your organization.

Trust Protection Platform's All Certificates dashboard has the Secure Protocols vs Insecure Protocols widget to help you quickly see certificates that may be putting your organization at risk with an insecure protocol.

This bubble chart shows secure protocols in green and insecure protocols in red. There may be multiple bubbles of each color, if you have connections for a certificate in your system with multiple protocols. A single certificate may be present in more than one bubble, depending on the validation information found for that certificate. For example, a certificate may be installed on two different devices that use different protocols. A device may be configured to allow multiple protocol versions, so the end point may appear in multiple bubbles.

Click a bubble to see a filtered list of certificates that match that bubble's protocol. You can also click on the description in the key to see a filtered list of certificates that match that protocol group. On the filtered results list, click the down arrow in the TLS Endpoints column to see protocol information.

Working with the User and Client Device Certificate (dashboard)

The User and Client Device Certificate (dashboard) is similar to the All Certificates (dashboard), but the User and Client Device Certificate (dashboard) shows only information about user and client certificates. All other certificate types are excluded from this dashboard.

The widgets on the All Certificates (dashboard) are listed on the right side of this page.

Client Certificate Totals Widget

The Client Certificate Totals widget gives you an overview of important certificate data and provides a quick way for you to access filtered lists of certificates in your inventory. This widget is comprised of pre-defined tiles that you can enable or disable as needed. Some of the tiles can be customized to fit your needs. Clicking the number in any tile opens a filtered list in the certificate inventory where you can view the certificates in detail.

Available tiles

- **Awaiting CSR.** Number of certificates waiting to be approved by a CA.
- **Distrusted Entrust.** Number of certificates issued by one of the following CAs:
  - Entrust
  - AffirmTrust

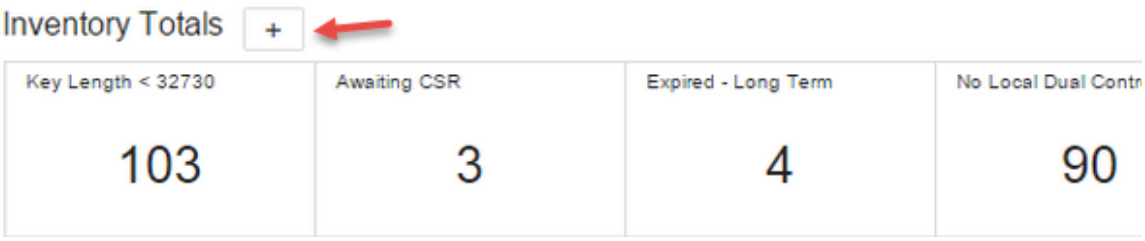
  Some web browsers flag these certificates as a potential security risk.
- **Expired < 30 days**. Number of certificates that expired less than 30 days ago. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 613.
- **Expired > 30 days**. Number of certificates that expired more than 30 days ago. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 613.
- **Expiring within 30 days**. Number of certificates that expire in the next 30 days. The 30-day threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 613.
- **Expiring - Second Half of the Renewal Period**. Number of certificates that are not renewed and that are past a given time period. Available options are:
  - Second Half of the Renewal Period
  - Final Quarter of the Renewal Period
  - Specific number of days after the Renewal Period starts.

  If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 613.
- **Failed Revocation.**
- **Failed Validation.**
- **In Error.**
- **Key Size < 1024.** Number of certificates that have a key size less than 1024 bits. The key size threshold is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on page 613.
- **Local Dual Control Needed.** Number of certificates that might not have a reviewer or approver with local knowledge.

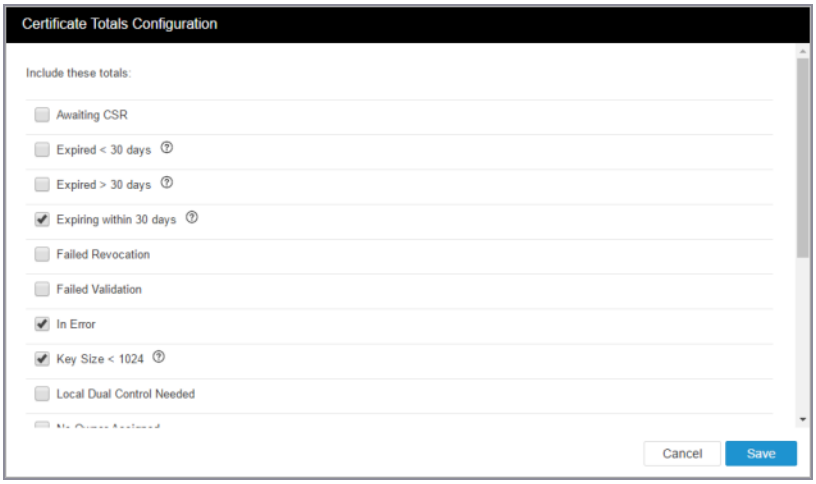
- **No Owner Assigned.** Number of certificates that have no assigned contact.
- **Pending My Approval.** Number of certificates that you need to take action on, because you have been assigned to approve them. These certificates may be in any state.
- **Total Certificates.** Number of certificates that you have permissions to, including Retired and Lost certificates.
- **Total Managed Certificates**. Number of certificates that you have permissions to, excluding Retired and Lost certificates.
- **Total Retired Certificates**.
- **Unapproved Issuer**. Number of certificates that have been issued by a CA that is not approved in Trust Protection Platform. To learn how to approve a certificate issuer, see Approving a certificate issuer (CA).
- **Validity Periods.** Shows the total number of certificates that exceed the default validity period (specified in days). The validity period is customizable. If you change the threshold value, the name of the widget will update accordingly. See "Configuring or editing a tile" on the facing page.
- **Weak Signing Algorithm**: Number of certificates not signed by one of the algorithms defined in Account Preferences. See "Configuring or editing a tile" on the facing page.

Adding tiles

1. Click + .



2. In **Widget Configuration**, select the tiles you want to add.



3. Click **Save**.

Removing Tiles

Hover over the tile you want to remove, and click the ✕ in the top right corner of the tile.

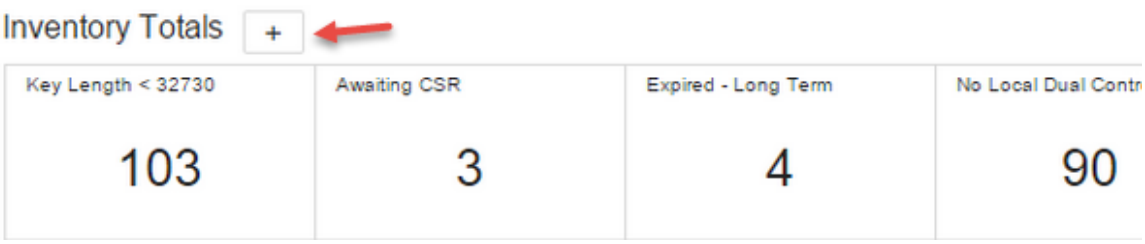
Reordering tiles

Hover the pointer over the tile until the pointer becomes ✥, then drag the widget to a new location.

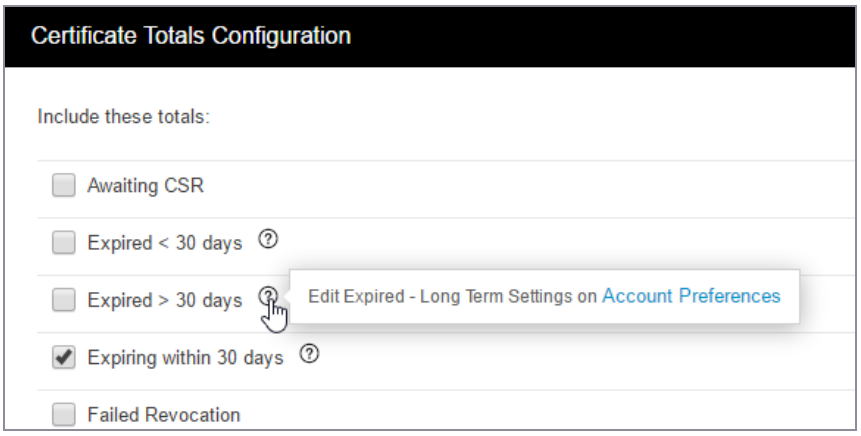
Configuring or editing a tile

A number of the tiles can be customized to show values that meet your specifications.

1. Click **+**.



2. Tiles that can be customized have a help icon ⓘ. If you want to edit the value of a tile, click the help icon, and then click the **Account Preferences** link. For more information, see "Configuring value thresholds using Account Preferences" on page 631.



Certificate Key Size widget

Certificates contain cryptographic keys that are used to protect information and/or authenticate users or devices.

The length of a cryptographic key determines how difficult it is to break. The U.S. National Institute of Standards and Technology (NIST) recommends that all organizations stop using keys that are less than 2048-bits for asymmetric algorithms (e.g., RSA, DSA, Diffie-Hellman) by the end of 2013.

Using the Certificate Key Length widget, you can easily identify keys in your environment that are smaller than 2048.

BEST PRACTICE To better secure and protect your environment, replace all certificates in which the key length is below 2048.

NOTE A key length of zero (0) indicates an ECC (Elliptic-curve cryptography) certificate.

Certificate Signing Algorithm Widget

Certificates are digitally signed by certificate authorities (CAs) to ensure their authenticity. Digital signatures are applied using message digest or hash algorithms (such as MD5 and SHA1) and asymmetric algorithms (such as RSA and DSA). They are typically named using a combination of each algorithm type, such as MD5RSA or SHA1RSA.

The National Institute of Standards (NIST) and other standards organizations provide guidance on algorithms that are considered secure. Use the Certificate Signing Algorithm widget to help ensure that your certificates are in compliance with their recommendations.

Certificate Protection Level widget

The Certificate Protection Level widget identifies certificates by management type. The management types are:

- **Unassigned**. These certificates are neither enrolled or monitored by Trust Protection Platform.
- **Monitoring**. These certificates are continuously monitored for expiration and associated risks.
- **Enrollment**. At this level, Trust Protection Platform interfaces directly with Certificate Authorities (CAs) to initiate and auto-enroll new or to-be-renewed certificates and key generation requests according to organization-defined workflow and approved policies.
- **Certificate Installation (Provisioning)**. These certificates are enrolled and automatically provisioned by Trust Protection Platform to web servers and appliances that use them.

For more information about these protection levels, see Certificate Management.

Certificate Validity Period widget

A certificate's validity period is the length of time that a certificate is valid for use. The longer a certificate is valid, the greater the possibility that the private key used with that certificate has been compromised.

Private keys used with certificates are susceptible to internal and external compromise. For example, in order to manage certificates, many administrators have direct access to private keys and can make copies of them. This represents a significant risk if an administrator is reassigned or terminated and the certificates and private keys they were managing are not replaced for an extended period of time.

Minimizing certificate validity periods helps ensure that certificates are replaced regularly. To reduce the risk of compromise, certificate validity periods of one year or less should be used.

The Certificate Validity Period widget helps you to easily identify the age of your certificates so that you can adhere to this best practice.

Certificate Authorities widget

This widget displays the number of certificates by the issuing certificate authority (CA), including self-signed certificates. This can help ensure that you are using CAs according to your own trust policies.

Certificate Expiration widget

Expired certificates create a serious threat. The Certificate Expiration widget helps you stay ahead of the risk curve by showing certificates that have upcoming expiration dates. You can customize the date range shown in the widget by clicking the date range drop-down box near the widget title. On the graph, you can hover over a bar to see the validity period for that bar and the number of certificates represented by that bar. Clicking the bar opens the Certificate Inventory filtered to just those certificates.

What do the colors mean?

The Certificate Expiration widget utilizes specific colors to make it easy to identify the state of each certificate.

Blue: Certificates that are in an expired state.

Red: A critical state showing certificates that either have already expired, or that will expire within the next 15 days or less.

Yellow: Indicates a less critical state showing certificates that will expire within the next 16 to 30 days.

Green: These certificates are considered secure because their expiration dates are out 30 days or further.

- To view details and to take action, click a bar.

Certificate Origin widget

The Certificate Origin widget displays the solutions that added certificates to the certificate inventory. It displays the total number of certificates added by each solution, and it also provides a percentage for each solution when you hover over the pie chart. Clicking a section on the pie chart opens the certificate inventory list filtered to the pie chart selection.

Certificate Trends widget

The Trends widget provides a burn-down chart view that can help you to easily identify trends within certificate management. Using the drop-down selectors at the top of the widget, you can select what trend you'd like to see and over what period of time you'd like to see it.

NOTE Widgets require some historical data in order to provide value. For example, the Trends widget cannot provide trending data about private key orphans until orphans have been found and tracked for at least a few days.

When the agent checks in with Trust Protection Platform and has changes to report, the graph is updated when any changes have been discovered by the agent.

The Trends widget on the User and Client Device Certificate (dashboard) lets you track the following key indicators:

Trend	Description
Key Size	Displays the trend for each key length from 512 up to 4096. This trend can help to identify when and to what extent weaker key lengths are being used.
Signing Algorithm	Displays the number of certificates grouped by Digital Signature Algorithms (signing algorithm), which can help you evaluate risk and company security policy compliance.
Key Algorithm	Shows the algorithm used to generate the key. RSA and ECC are the two types of algorithms used.
Management Type	Displays the number of certificates by management type over time. Management types include: ■ **Monitoring** ■ **Enrollment** ■ **Provisioning** ■ **Unassigned**: Unlicensed Trust Protection Platform certificates and keys that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.
Issuer	Displays certificates by their originating CAs, including self-signed certificates.

Validity Period	Displays the number of certificates by validity period, or the amount of time before certificates expire (0 to 1 year, 2 years, and 3 years, respectively).
Certificate Type	Shows the types of certificates: Device User.
Total Certs	Indicates the total number of certificates under Trust Protection Platform management.
Renewal	Shows the number of renewals that are going to happen on each calendar day that is displayed in the widget.
Certificate Origin	Shows the total number of certificates issued per solution. This option is available only if Client Protect is licensed.
Protection Status Summary	The difference between the graph line showing the total number of certificates and the line showing the total number of secured certificates provides a clear view of how secure your certificate inventory really is.

Working with the SSH Keys (dashboard)

Detection is a critical component of trust. If you are unaware that a compromise has occurred, you cannot respond. Trust Protection Platform provides visibility into your entire SSH key (and certificate) environment.

The SSH Keys (dashboard) offers several widgets designed to give you current and relevant insight into potential SSH key vulnerabilities.

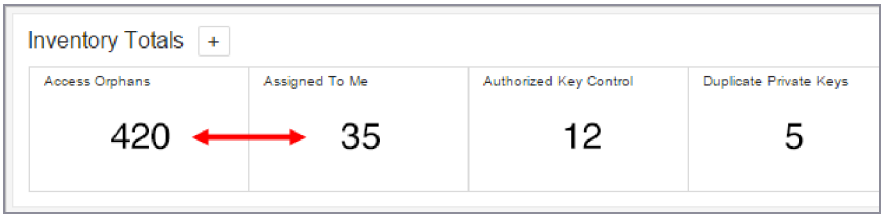
The SSH Keys (dashboard) provides a customizable view into the state of your trust environment. Depending on your roles and responsibilities, you can add or remove special widgets that show you information that is relevant to you.

Reducing information clutter improves your ability to both detect and respond to anomalies and threats. And the ongoing monitoring of key and certificate usage lets you know when a key or a certificate is being used by someone other than the person to whom it was prescribed.

Key Totals widget

The Key Totals widget gives you the most important information on data counts in your network. This enables you to quickly assess your SSH inventory.

TIP You can drag and drop tiles to reorder them.



Default tiles

Several tiles are displayed by default.

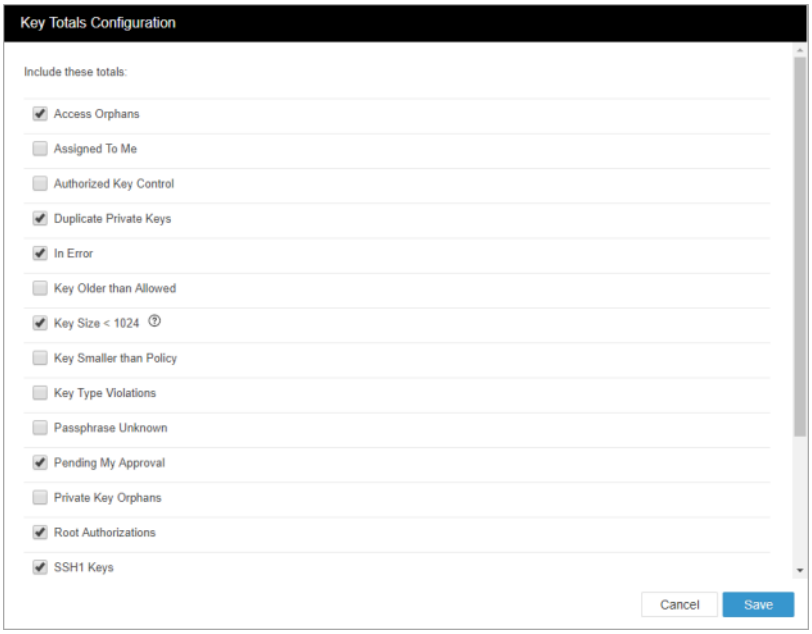
- **Total Keys-** Total number of keys
- **Access Orphans -** All keys with *Client Access Orphan* or *Root Access Orphan* status. For more information, see Client and root access orphans.
- **Root Authorizations -** All keys with the *Root Access*or *Root Access Orphan* status. For more information, see Remediating root access violations.
- **Duplicate Client Private Keys -** A duplicate client private key is compliant if the policy setting for *Allow Duplicate Private Keys* is set to *Yes*. If the setting is *No*, then the duplicate private key is non-compliant. One example where this might not be a risk is if a client private key is in multiple places on the same device.
- **Duplicate Host Private Keys -** A duplicate host private key is compliant if the policy setting for *Allow Duplicate Private Keys* is set to *Yes*. If the setting is *No*, then the duplicate private key is non-compliant.
- **SSH-1 Keys -** The SSH1 protocol is highly vulnerable and is an extreme risk for organizations that use it. A design flaw in the SSH-1 protocol allows a malicious server to establish two concurrent sessions with the same session ID, allowing a man-in-the-middle attack.
- **Key Size < 1024 -** Any asymmetric keys using an encryption length that is less that what you have specified in the associated policy. You can configure an account preference to bring keys into compliance with your key length requirements. For more information, see "Configuring value thresholds using Account Preferences" on page 631 in the Administration Guide.
- **In Error -** All keysets with the *Rotation Failed* status
- **Pending My Approval -** Number of keys in a workflow state that requires your action for approval. Approval may be required for certain key actions like provisioning, editing, or deleting a key. For more information, see SSH Keys workflow overview.

Adding or removing a tile

1. Click the **plus button** next to **Inventory Totals**.



2. In **Configuration**, select the tiles you want to add.



3. Click **Save**.

To configure or edit a tile

You can configure these tiles:

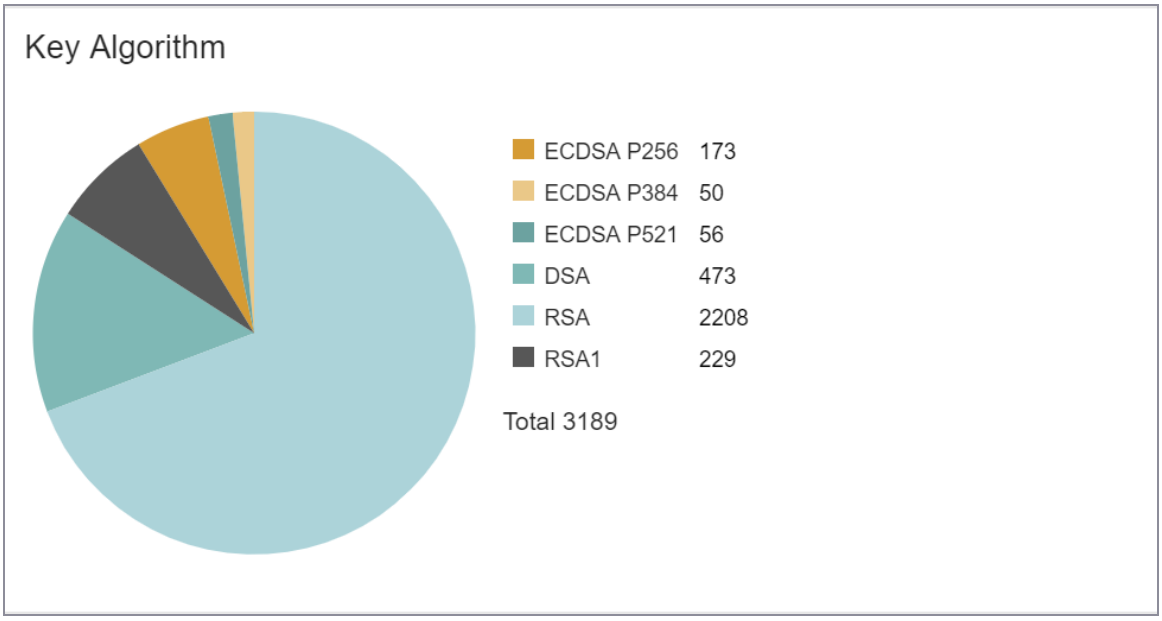
- Key size < 1024
- Unused Authorized Keys

See "Configuring value thresholds using Account Preferences" on page 631 in the Administration Guide for information on how to make changes.

SSH key algorithm widget

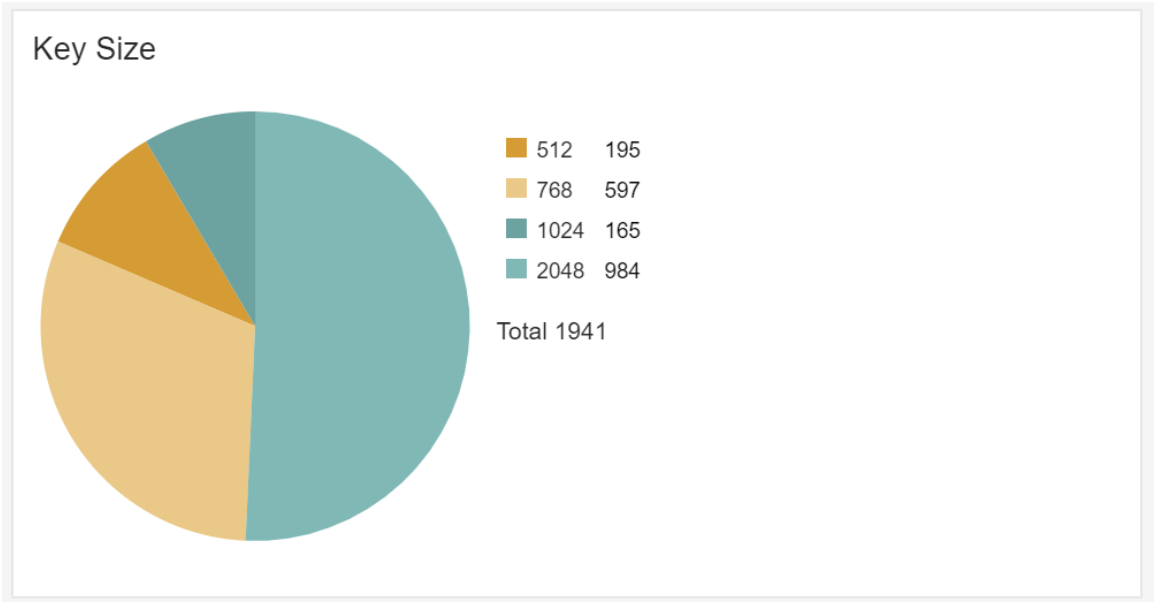
This widget is useful for quickly identifying the number of keys encrypted using available algorithms.

Trust Protection Platform can discover DSA keys, and both discover and generate keys using RSA/RSA1 key encryption algorithms.



Key Size widget

The length of a cryptographic SSH key determines how difficult it is to break. Using the Key Size widget, you can easily identify SSH keys in your environment that are smaller than 2048.

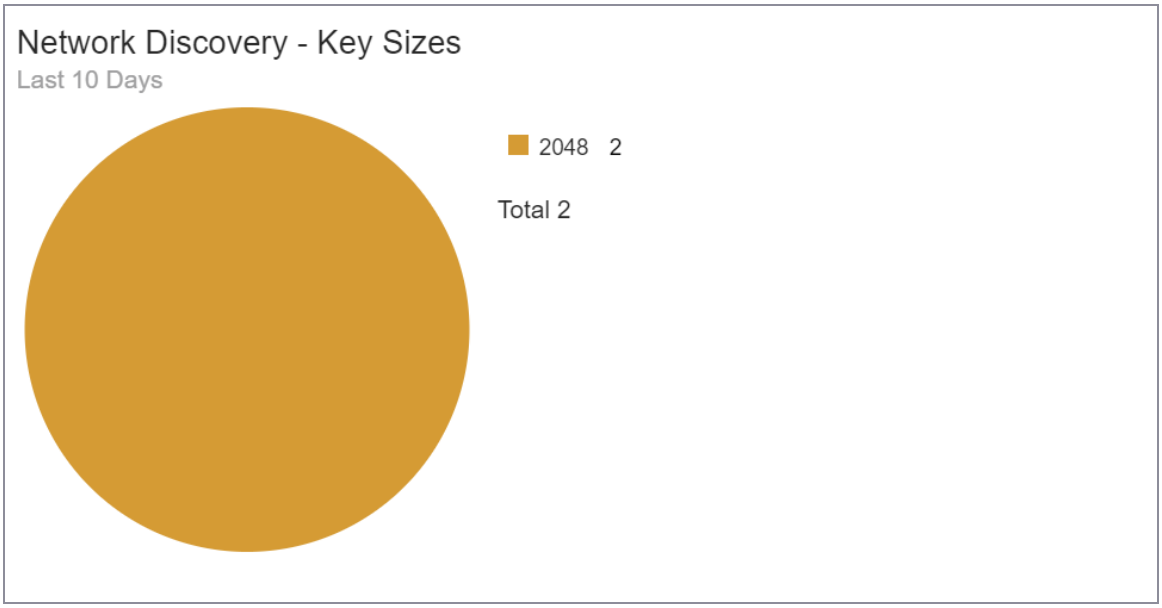


BEST PRACTICE To better secure and protect your environment, the National Institute of Standards and Technology (NIST) recommends that you use 2048 or higher encryption when using RSA.

Network Discovery–Key Size widget

The Network Discovery Key Size widget lets you rapidly assess security risks related to weak key lengths based on the results of network discoveries.

At a glance, you can identify the total number of SSH server keys for each distinct key length (e.g., 768, 1024, 2048 bits). Trust Protection Platform includes results for SSH keys in all network discovery queues in the discovery tree.



Trust Protection Platform's network discovery keeps a record of all keys that were discovered, even if they haven't been seen in a recent discovery scan.

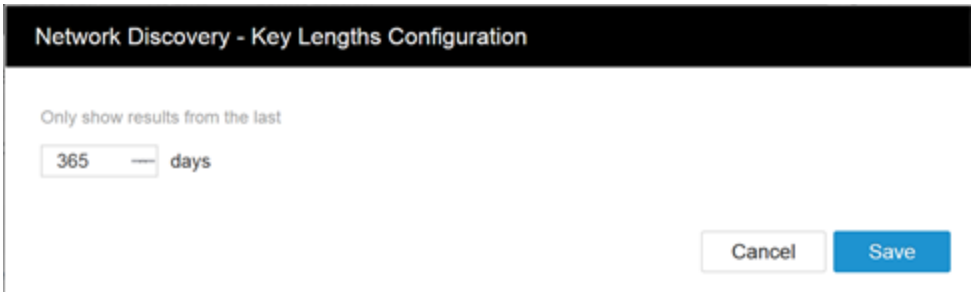
To track when each key was last seen, Trust Protection Platform updates the Last Seen On date for each key that is discovered during a scan. You can configure the window of time within which you would like to see results.

EXAMPLE If you configure the *Only show results from the last option* to 90 days, the widget only shows statistics for keys that have been discovered in a scan within the last 90 days.

The default for this option is 365 days.

To customize displayed results

1. Move your mouse cursor over the Network Discovery Key Lengths widget and click ⚙ to open the widget's **Properties** box.
2. In the **Only show results from the last** field, type a number (in days).



3. Click **Save**.

BEST PRACTICE Cryptographers have been making steady progress in factoring larger and larger key lengths. 512 bits is more easily factored today and the factoring of 768 bit keys has also been demonstrated. These are publicly known factoring capabilities. However, there are likely more sophisticated organizations that have successfully factored even larger key lengths. Therefore, it is critical to have an inventory of all of your keys and to ensure that key lengths at least match the National Institute of Standards and Technology (NIST) recommendations.

Network discovery and the SSH Network Discovery Key Lengths widget enable you to quickly detect weak server keys in your environment so that they can be remediated.

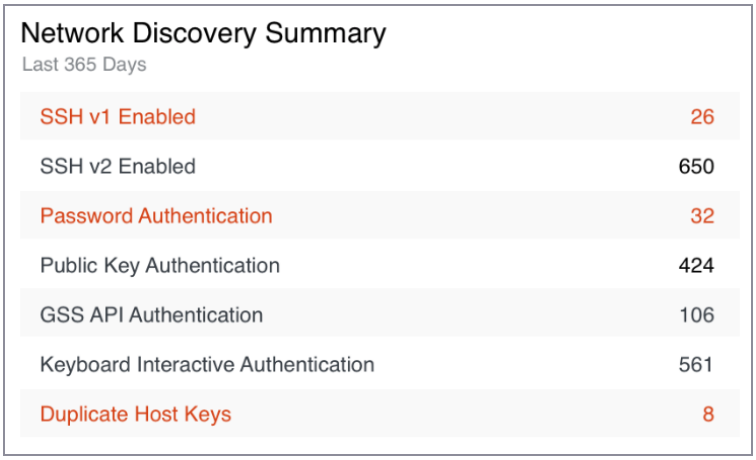
SSH Network Discovery Summary widget

This widget provides critical information related to your SSH servers and the kinds of authentication methods being used.

It helps you to rapidly assess security risks based on the results of network discoveries. The widget displays the total number of SSH servers, protocol versions currently in use, and the authentication methods that are enabled on those servers.

For example, at a glance, you can identify how many SSH servers have been discovered in your network, and of those discovered servers, how many allow the use of SSH version 1 (SSH1) and SSH version 2 (SSH2).

Perhaps you have an established policy to allow only public key authentication (no password authentication). The Network Discovery Summary widget gives you a summary of the number of servers that have each possible authentication method enabled so that you can align your servers with your organization's security policy.



About Network Discovery

Trust Protection Platform network discovery keeps a record of all SSH servers that were discovered, even if they haven't been discovered during recent scans. To track when each key was last found, Trust Protection Platform updates the Last Seen On date for each key that is discovered during a scan. You can configure the window of time within which you would like to see results. For example, if you set the **Only show results from the last** option to 90 days, the widget only shows statistics for servers that have been discovered in a scan within the last 90 days. The default setting for this option is 365 days.

To set this value, click the configuration cog in the upper right hand corner of the widget, specify the number of days, and then click **Save**.



BEST PRACTICE SSH1 is known to have security vulnerabilities that can be exploited by attackers if it is enabled for use on SSH servers. SSH2 addresses these vulnerabilities. Either without realizing it, or sometimes for backwards compatibility, administrators in your organization might have enabled SSH1 on some servers. It is critical that you identify all servers that have SSH1 enabled, determine if it is required for backward compatibility with legacy applications and then either disable it or take steps to minimize the potential for exploits (for example, by limiting network access to the affected systems).

Network discovery is a good method for quickly identifying where SSH servers are deployed in your environment. After you know where they are deployed, you can then ensure that agents are deployed on those systems and that all keys are discovered and accounted for.

The SSH Network Discovery Summary widget provides the following information:

- **SSH Servers**: Shows the total number of SSH servers discovered using Trust Protection Platform's network discovery.
- **SSH v1 Enabled**: Shows the total number of servers that have SSH1 enabled. This is considered a risk, and will appear in red if there are 1 or more.
- **SSH v2 Enabled**: Shows the total number of servers that have SSH2 enabled.
- **Password Authentication Enabled**: Shows the total number of servers that allow password authentication (PasswordAuthentication). This is considered a risk, and will appear in red if there are 1 or more.
- **Public Key Authentication Enabled:** Shows the total number of servers that allow public key authentication (PubkeyAuthentication).
- **GSSAPI Enabled**: Shows the total number of servers configured to use Kerberos (GSSAPIAuthentication) for authentication.
- **Keyboard Interactive Authentication**: Shows the total number of servers configured to use keyboard interactive authentication (ChallengeResponseAuthentication), and can be used to prompt users for information.

  NOTE If the host advertises that it supports *password* and *keyboard-interactive* authentication, then *password* will always be chosen. If *password* is not advertised, but *keyboard interactive* is, then Trust Protection Platform falls back to the expected username and password prompts (unless otherwise configured.)

A note about Centrify and Solaris SSHD authentication[1]

- **Duplicate Host Keys:** Shows how many duplicate host keys have been discovered across your environments. This is considered a risk, and will appear in red if there are 1 or more.

Click any item on the widget to see the SSH Network Discovery Report, where you can see the specific servers for each widget entry. For more information, see Analyzing the SSH Network Discovery report.

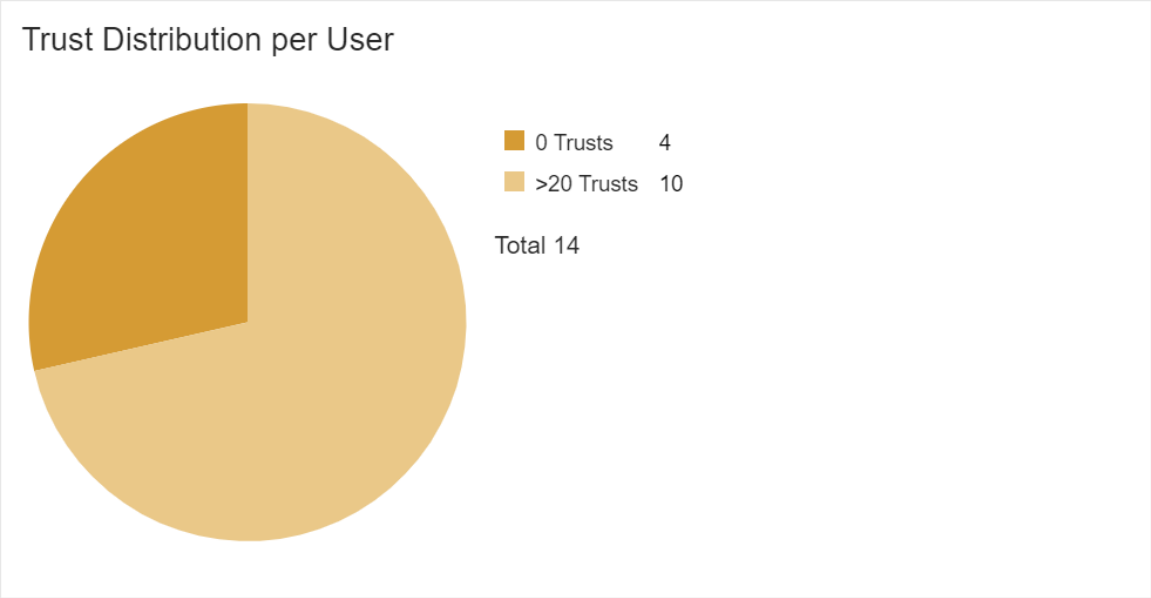
You can get more details about the SSH servers and enabled protocols and authentication methods by looking at the **Discovery** tree in Policy Tree.

> **TIP** By default, *keyboard interactive authentication* typically implements password authentication in a single challenge-response cycle, simply prompting the user for a single password. However, this can be confusing because it looks very much like *simple password authentication*. If you're not deliberately using both for different purposes, consider disabling one or the other to avoid end-user confusion.

Trust distribution per User widget

For any single user to be given trust across dozens of servers is typically a warning sign. One to three user trusts is common and probably acceptable. But when a single user shows a greater number of trusts, you should investigate and consider revising your user trust strategy.

[1] An issue has been reported with Centrify not working well with Solaris SSHD when *password* authentication is used. The work around is to enforce *keyboard interactive* authentication by changing **Password Authentication** to "no", and recycling SSHD.



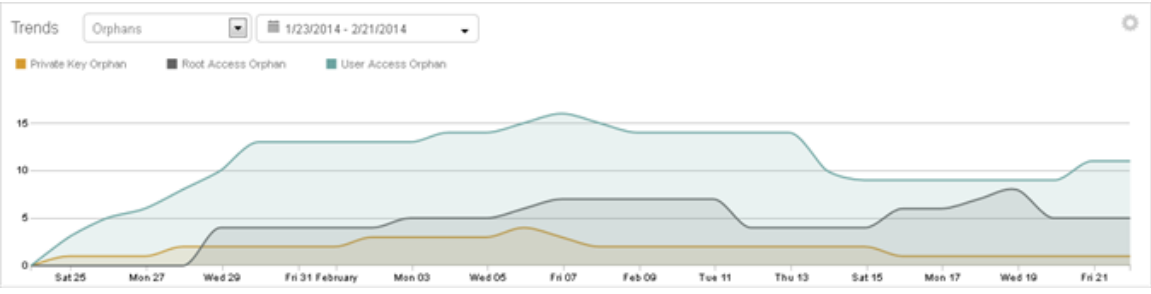
This widget identifies the number of trusts per user so that you can easily identify occurrences where an unusual number of trusts have been granted to a single user.

SSH trends widget

The SSH Trends widget provides a burn-down chart view that can help you to easily identify trends in your SSH management.

> **NOTE** Widgets require some historical data in order to provide value. For example, the Trends widget cannot provide trending data about private key orphans until orphans have been found and tracked for at least a few days.

When the agent checks in with Trust Protection Platform with changes to report, the graph is updated when any changes have been discovered by the agent.



The Trends widget lets you track the following key indicators:

Trend	Description
Orphans	Shows the increase or decrease of orphaned keys.
Non-Compliant Hosts	Servers containing authorized keys that are not in compliance with a defined policy. A single, non-compliant SSH key could open the door to unauthorized access to your server.
Non-Compliant Keys	
Agents	Shows the number of agents that are authenticating and reporting into Trust Protection Platform.
Duplicate Private Keys	Indicates the number of allowed and not allowed private keys, and the number of private keys per user.
Policy Violations	Shows violations of policies that you have defined. For example, Trust Protection Platform detects keys that are not of the type you specified in a policy; or keys that exceed a validity period (old keys) specified in your policy.
Key Lengths	Lets you track progress in increasing key lengths to meet your policy. For example, you might be replacing 768 bit keys with 2048 bit keys. The Trend graph quickly reveals your progress toward meeting that policy.
Algorithms	Quickly see your progress in meeting algorithm policies by removing those that don't meet the criteria of your policy (for example, removing RSA and replacing with RSA1).
Vendor Formats	Identifies the use of various vendors over time (OpenSSH, Tectia, and PuTTY) to help you meet your vendor policies. For example, you might have decided to support OpenSSH and to remove your dependencies on Tectia. This graph can quickly show your progress by revealing the number of instances of each over a period of weeks.

Working with the System Status (dashboard)

The System Status (dashboard) gives you information about license counts and engines (a.k.a. Trust Protection Platform instance) that is connected to the Trust Protection Platform database.

> **NOTE** To use the System Status (dashboard), you must have View/Read permissions to the root of the Platform tree. For more information about setting permissions, see "About Permissions and Inheritance" on page 716 in the Trust Protection Platform Administration Guide.

License Counts

The License Counts widget gives you a quick view into the number of license-related items that are being tracked by Trust Protection Platform. Hover over a widget for additional information about each item.

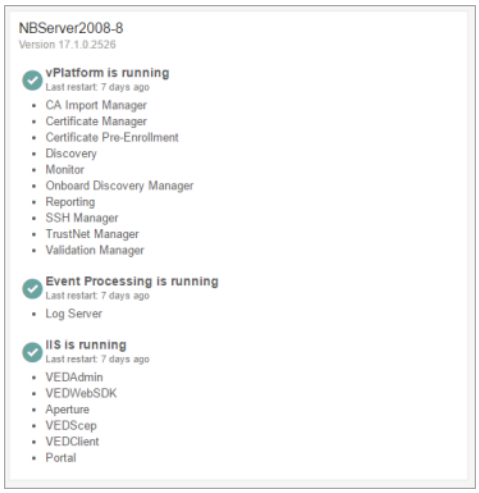
You can download a PDF or CSV copy of the license report using the **Download Report** button.

For more detailed information about what license-related items are tracked and reported by Trust Protection Platform, see Venafi License Report in the Reporting Administration guide.

> **NOTE** This data is not dynamically generated. The data reflects the information in the most recently-run license report. To update this data, re-run the Venafi License Report using the **Run Report** button.

Only users who have view/read access to the license report will be able to see the License Counts section on the dashboard.

Engine Connections



Each engine widget on the screen represents a separate Venafi Trust Protection Platform server that has been connected to the database via Venafi Configuration Console. The title of the widget is the name of machine that is connected. Beneath the title is the version number, so you can see what version of Trust Protection Platform is being used to connect.

The sections on the widgets show which services are running or not running. When services are up, you can determine the up-time of the service by looking at that last restart information. When a service is down, you can see how long the service has been disconnected.

The information for the IIS service can only be determined when vPlatform is running. If vPlatform is down, IIS will report status as "Unknown" and say that "vPlatform is required to monitor IIS."

To maximize system performance, vPlatform and the Event Processing engines only report updates to the database every five minutes. If no system status has been reported for six minutes or more, the service is considered to be down.

Trust Protection Platform includes a 'demo mode'. When enabled, the service information will update every 30 seconds, and will be considered down if a system status update has not been received for more than 45 seconds.

If you disable or delete a vPlatform component, that component will no longer appear in the widget. If you delete an IIS application pool, it will no longer appear in the IIS section of the widget.

The information from the System Status dashboard is also available via the WebSDK. For more information see GET SystemStatus in the WebSDK Developer's Guide.

When you retire a Trust Protection Platform server, you need to delete the engine from the Platform Tree in the Policy Tree before the engine's widget will be removed from the System Status dashboard and the WebSDK results.

Configuring value thresholds using Account Preferences

Throughout Venafi Platform, the system shows you information based on thresholds that you create to ensure you are protecting your key and certificate data in accordance with your organization's policies and objectives. Venafi Platform is designed to give you flexibility in providing warnings based on thresholds you define. These thresholds affect not only the data you see across the dashboards, but also apply to the way keys and certificates are reported to you throughout Venafi Platform.

Users can access the Account Preferences screen to configure these thresholds for themselves. Additionally, system administrators can set and lock values, so all users in the organization must use the same settings.

Setting threshold values for an individual

1. On the menu, click the user icon, then click **Preferences**.
2. From the left, select a product (TLS Protect & Client Protect; SSH Protect; or CodeSign Protect) depending on which settings you with to modify.
3. Modify the threshold values as needed.
4. Click **Save**.

Setting threshold values across the organization

1. Log in as the master admin.
2. On the menu, click on the user icon, then click **Preferences**.
3. From the left, select a product (TLS Protect & Client Protect; SSH Protect; or CodeSign Protect) depending on which settings you with to modify.
4. Modify the threshold values as needed.
5. Click the lock icon  to prevent others in your organization from setting a different personal value. If the value is locked, and you want users to be able to configure this value for themselves, click the unlock icon  .

   > **NOTE** Modifying these values without locking them will only modify them for your account, not for other users in your organization. Locking these values locks the value for all users.

6. Click **Save**.

TLS Protect and Client Protect settings

Name	Default	Description
Flag certificates which use a key algorithm with a strength of	80 (bits)	For some key types, smaller key lengths are less secure, You can choose to flag and report certificates that use shorter key length algorithms. This value is stored in bits.
Flag certificates with a validity period greater than	397 (Days)	Certificates with long validity periods may be more susceptible to being compromised. Set this value in days. (The default is 397 days.)[1]
Weak Signing Algorithm	None	Allows and reports algorithms considered to be less secure or outdated for signing operations.
Flag certificates as Expired - Long Term if expired for longer than	30 (Days)	Expired certificates are grouped into two categories: (1) Expired - short term; and (2) Expired - long term. This helps you with analysis and reporting to recognize items that have recently expired so you can take action on them, if necessary. Set this value in days.
Flag certificates as Expiring Soon if expiring in less than	30 (Days)	To give you enough time to take action on a soon-to-expire certificate, the system begins warning you before a certificate will expire. This value controls how early you want to be alerted to expiring certificates. Set this value in days.
Support Large Object Trees	No	Setting to "Yes" will force all users' administration consoles to launch in query mode. See "Start the console in Query mode" on page 41

[1] In version 20.3 and older, the default value was 820 days, however the major browser vendors no longer accept public certificates with a validity period longer than 397 days. If you had a version of Venafi Platform earlier than 20.4 and you *left this value at the default*, upon upgrade to 20.4 (or later) the new default of 397 days will apply. However, if you had customized this value, upon upgrade to 20.4 (or later) your *previous custom value* will be used.

SSH Protect settings

Name	Default	Description
Flag certificates which use a key algorithm with a strength of	80 (bits)	For some key types, smaller key lengths are less secure, You can choose to flag and report certificates that use shorter key length algorithms. This value is stored in bits.
Flag keys as Unused Authorized Keys if not used for	365 (Days)	SSH Protect tracks authorized key usage. If an authorized key has not been used for a long period of time it may be time to remove the key so it no longer has any access to your systems. This helps protect your system so old keys can't be used to access the system by somebody who is no longer authorized to have access. Set this value in days.

CodeSign Protect settings

On the CodeSign Protect User Preferences, you can re-enable the First Project dialog, as if you are logging into the product for the first time. Click **Clear Setting** to see this dialog again.

11

Working with identities, permissions, and teams

In Trust Protection Platform, access to the system is managed primarily through identities. The term *identities* refers to both users and groups in the system. Roles with specific permissions are also used and can be assigned to both users and teams (see "Understanding system roles" on page 706).

Identity information can be obtained through several sources including external data sources, as well as locally-created and managed users and teams. Identities control access not only to the overall platform, but through inheritance policies that can be controlled at all levels of your data structure, all the way down to the individual items being tracked in Trust Protection Platform.

This chapter includes information about how to manage identities and the permissions associated with identities. This information is organized into the following main groups of information:

- **Managing identities from third-party data providers.** Most organizations manage their users and groups in systems like LDAP or Active Directory. You can synchronize the data in Trust Protection Platform with your identity provider, and assign permissions to users and groups imported from your external data source.
- **Managing identities directly in Trust Protection Platform.** These identities are called *local identities*. You can create, organize, and manage users and groups directly in the system, and assign permissions accordingly.
- **Managing permissions for identities.** The permission management system works the same way regardless of whether your identity information is imported from a third-party source, or whether the

identities were created directly in Trust Protection Platform. In this section, you will see how permissions are granted and managed across the various Trust Protection Platform consoles.

- **Searching for identities.** If you need to see what permissions are granted to an identity, there are a couple of ways you can search for them in Trust Protection Platform, giving you a clear view into what users and groups are in your system, and what permissions they have.

All users shown in the system can log in to Trust Protection Platform; however what they can *see* and *do* depends upon their assigned permissions. Trust Protection Platform uses a *least privileged* model of system administration. So, by default, local users (users created directly in Trust Protection Platform) have only the *Read* permission and external users (those imported into Trust Protection Platform from a third-party data source) have no permissions. You must explicitly grant permissions to users and groups before they can manage objects.

Managing identities from third-party data providers

Most organizations already have an authoritative source for user and group information that is managed by the organization. Trust Protection Platform can integrate with external data providers to synchronize user and group information between Trust Protection Platform and your authoritative identity source.

This section includes information you need to connect and manage identity information between Trust Protection Platform and your external data source.

Working with Active Directory

One of the most common external identity providers is Microsoft's Active Directory(AD). Trust Protection Platform connects to AD, importing users and groups into Trust Protection Platform. You can connect to your Active Directory source via an IPv4 or an IPv6 connection.

Typically, Active Directory connections are read-only. Trust Protection Platform reads the User and Group data directly from Active Directory in real time so you can log in as an external user, view external users and groups in the Identity tree, select external users or groups as object Contacts, and assign object permissions to external users and groups.

Requirements for creating an Active Directory connection

The Active Directory (AD) Wizard lets you create and configure Active Directory connections. For the provider to establish a connection to Active Directory, you must provide the following:

- **Active Directory service account** Account credentials that can be used for Active Directory authentications. This account must:
  - Have the required permissions to access the Active Directory forest or domain(s) that you want to include in the connection.
  - Be provided in User Principal Name (UPN) format (administrator@example.com).
- **Host** The connection provider can resolve the following address types:
  - The host name must be provided as a fully qualified domain name (FQDN).
- **Host name for the forest, domain, or domain controller** For a forest or domain, the provider enables access to the forest or domain hosted at the address, and also discovers trusts that enable access to objects based on the search roots you select in the wizard.

  For a domain controller, the provider enables access to the domain hosted at the first resolved IP address.
- **Forest or domain name** If the provider attempts to resolve the host and discovers more than one Active Directory service, you are prompted to select the service you want to use. For example, if the provider analyzes the host and discovers both a forest and a domain, the wizard prompts you to select one of the them.

  Venafi recommends not creating Active Directory connections that overlap. In some cases, the provider cannot resolve the Trust Protection Platform user's permissions assignment properly. An example of overlapping connections is Active Directory connection #1 includes domain A which has a trust relationship with domain B, and Active Directory connection #2 includes domain C which also has a trust relationship with domain B.
- **Active Directory connection type** The type will either be Simple or Secure (default) based on your Active Directory implementation. This configuration determines the LDAP protocol bind type that the connection provider uses to communicate with Active Directory.

Cloud Active Directory Providers

Azure Active Directory Domain Services and *AWS Managed Microsoft AD* are considered compatible with Trust Protection Platform.

The same requirements listed above also apply to cloud Active Directory providers.

NOTE In Trust Protection Platform, user directories are closed systems. This means that local users can see only local users and groups. Likewise, external users can see only external users and groups within their own directory (or, if enabled within their own directory and the local directory). For example, if you have three LDAP connections, you must log in to LDAP1 to see its contents, LDAP2 to see its contents, and LDAP3 to see its contents.

For information about allowing external identities to see local identities, see "Allowing AD and LDAP users to see teams and local users" on page 688.

Additional configuration options for the Active Directory connection

In the wizard or after the Active Directory connection has been created, you can configure the following options:

- **Global catalogs & Domain Controllers**- If the Active Directory host has referral access to any global catalogs, they will be discovered and used automatically without any interaction required on your part. The same is true for domain controllers. This allows you to add or remove global catalogs and domain controllers without worrying about causing an outage in Trust Protection Platform. For more information, see "Automatic configuration of domain controllers and global catalogs" on page 672.
- **Search roots** - During configuration, you must select one or more search roots that contain the identities you want to be able to access using Trust Protection Platform. By selecting search roots, you can purposely omit Active Directory folders that you do not want to be able to access using Trust Protection Platform.
- **Nested group resolution** - You can configure the Active Directory connection to resolve nested groups.

  The provider can resolve groups and group members if the forest or domain has a trust relationship with the forest or domain to which the group or group member belongs. Nested groups are expanded until the provider encounters a group that belongs to a different forest, even if a trust exists. This functionality applies to Trust Protection Platform's e-mail notifications, approval requests, and reports, and also to a Trust Protection Platform user's ability to browse the objects that are included in the Active Directory connection.
- **Trusts** - Trust Protection Platform honors trust relationships in Active Directory, and allows you to access objects in other forests or domains that have an existing trust with the source forest or domain.

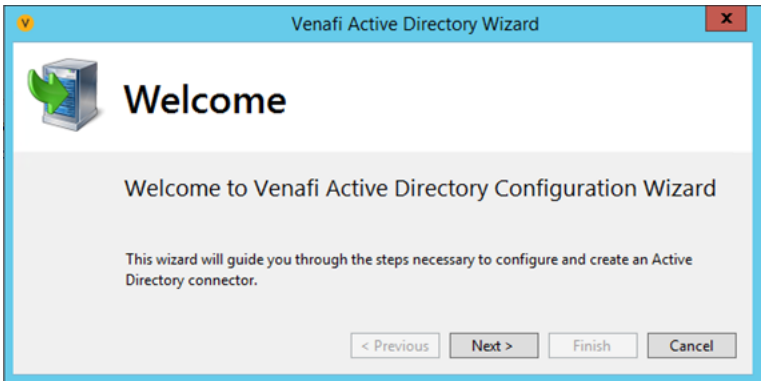
Creating an Active Directory connection

You can use Venafi Configuration Console to create and view Active Directory connections. Trust Protection Platform can connect to Active Directory via an IPv4 or IPv6 connection. You can create multiple Active Directory connections as necessary.

The Active Directory Connection integrates Trust Protection Platform with an Active Directory tree. The connection allows Trust Protection Platform to read User and Group data directly from Active Directory. So, you can log in as an external user, view external users and groups in the Identity tree, select external users or groups as object Contacts, and assign object permissions to external users and groups.

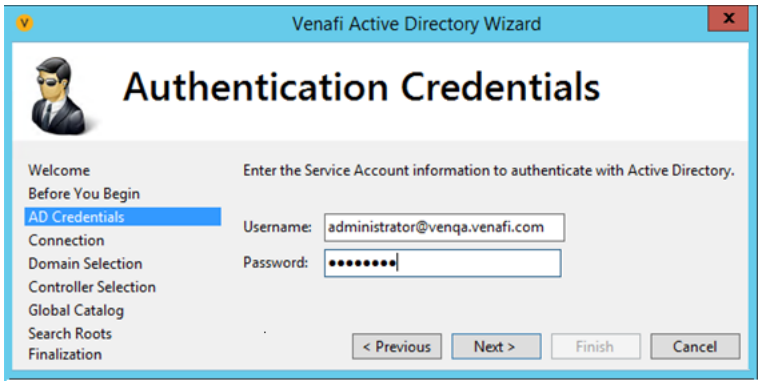
To create an Active Directory connection

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the left pane of VCC, click **Connectors**.
4. In the right **Actions** pane, Click **Active Directory Connector**.
5. If prompted, log in with your Trust Protection Platform local, master administrator credentials.
6. On the Welcome page, click **Next** and then log in with your credentials.



7. On the **Before You Begin** page, read the requirements. Be sure you know the AD root you want for the Root Selection step. Click **Next**.
8. On the **Authentication Credentials** page, type the credentials for the Active Directory service account, and then click **Next**.

   The username must be in the User Principal Name (UPN) format. For more information, see "Requirements for creating an Active Directory connection" on page 636.

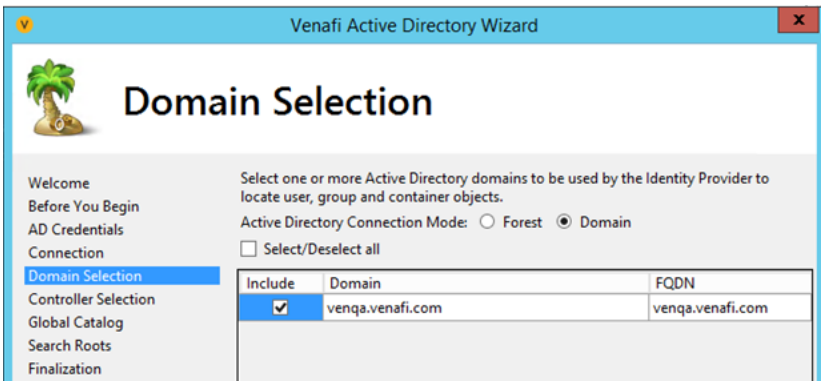


9. On the **Connection** page, enter the following information, and then click **Next**.

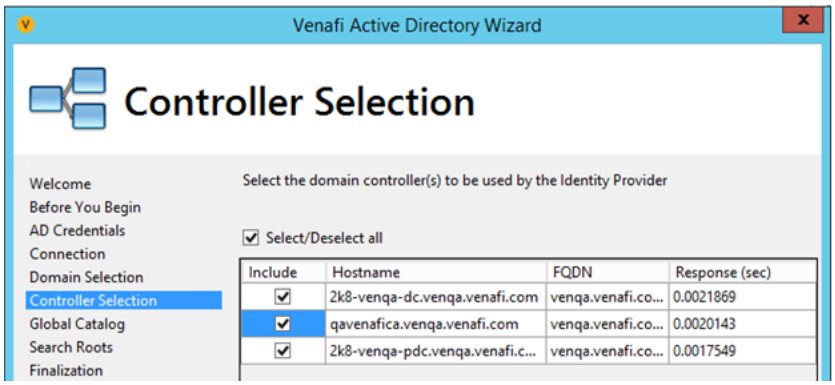
Parameter name	Description
Name	The Fully Qualified Domain Name (FQDN) of the AD host where Trust Protection Platform will connect and access Active Directory user domains, and then click **Next**. For example, host.example.co.
Connection	The managed AD directory: ◦ **Simple**: An unencrypted connection. ◦ **Secure**: An encrypted connection.

Parameter name	Description
Concurrency	The number of processing threads to use for searching for users in the identity provider.
Choose Domains and Controllers Specific to this Platform	When selected, the settings you apply on the following screens will apply to this Venafi Platform server only. This allows you to have AD connectors in different security zones or segments in your network. When checked, the next box, "Disable Rediscovery for This Platform" will automatically be checked, and will be disabled, as it is required when you choose domains and controllers specific to this platform.
Disable Rediscovery for This Platform	If you are not choosing domains and controllers specific to a platform, leave this option **unselected** (which will leave rediscovery enabled) unless told to disable by Venafi Customer Support. This box will automatically become selected and disabled if the previous option, "Choose Domains and Controllers Specific to this Platform," is enabled.

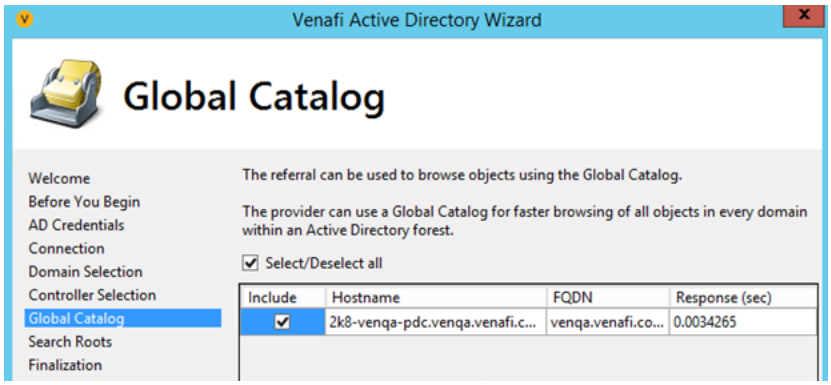
10. On the **Domain Selection** page, select the domains or forests to include, then click **Next**.



11. On the **Controller Selection** page, review the discovered domain controllers, and verify the correct controllers are selected for this network segment, then click **Next**.

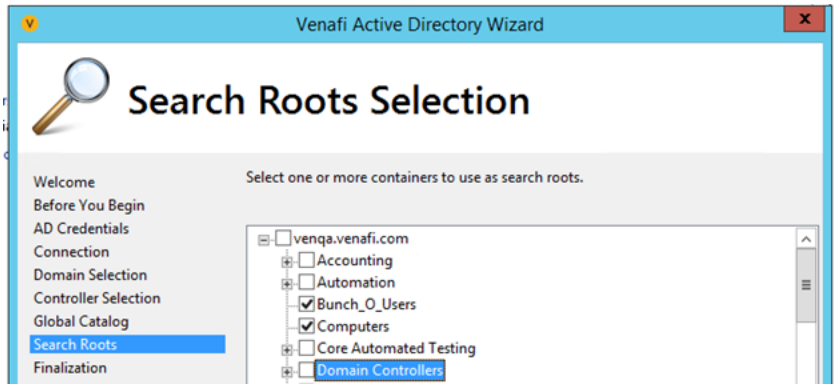


12. (Optional) On the Global Catalog page, review the discovered global catalogs, then click **Next**.



13. On the **Search Roots Selection** page, select the containers, and then click **Next**. If an error occurs, try the Common Name (CN) that appears in the error message as the container name.

    Select nodes or containers where users connecting to Trust Protection Platform are found. If the users are in a node that is not selected, they will not be able to authenticate with Trust Protection Platform.



14. On the Finalization page, specify the following, and then click **Finish**:

Parameter name	Description
Object Name	Object Name that will appear in the Trust Protection Platform Identity tree.
Friendly Name	A friendly name for the AD connection. This is part of the Prefix for the identity connector. The complete Prefix will end up as AD+FriendlyName. This name should be easy to use and remember. A prefixed name, for example the AD+FriendlyName, is one of the allowed login formats.
Resolve Nested Groups	(Optional) The provider expands nested groups while processing notifications.
Rank	(Optional) The order the Identity connectors are searched when looking for users. For example, let's assume the username is Bob. If there is a username called Bob in the local identity system and the AD connector, we set the identity connector to tried first. Most likely, it is the AD connector, which means the AD connector needs to have a lower rank (highest priority). You would set the rank for the AD connector to **0** and the Local identity connector to **1**.

What's next

1. Restart the Trust Protection Platform and Venafi Log server.
2. Restart server services on all Trust Protection Platform servers.
3. Restart the IIS web server on all applicable Trust Protection Platform servers.
4. To review or update basic settings from VCC, click **Properties**.

Viewing Active Directory configuration settings and mapping rules

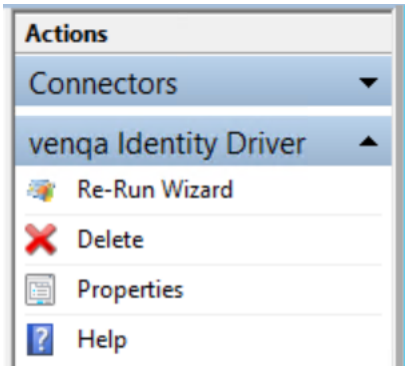
You can view and edit an existing Active Directory object in the following ways:

- To edit: In the Venafi Configuration Console, go to the **Connectors** node, click on the connector you want to edit, then click **Re-Run Wizard**.
- To view: Open the Policy Tree. From the Identity tree, open the **Provider** tab of the Active Directory object. The following table shows you the information you can see in Policy Tree:

Tab	Sub-tab	Configuration settings
Provider		
	Settings	**Settings section:** Lists the name and friendly name of the AD connection, as well as the user name used to connect. Here you can also see the secure setting, as well as if nested groups are expanded by default. This section also shows you whether global rediscovery is enabled or disabled. To change this setting, modify the properties for the identity provider in the Venafi Configuration Console. See "Creating an Active Directory connection" on page 638 for more details. **Default section:** Shows the default configuration that all servers use unless a custom configuration is shown for a specific server (which is listed below.) Settings for individual servers override those in the Default section. These default settings include the global catalogs, domains, and whether rediscovery is enrolled. **Additional Information:** ◦ Each engine that is using a unique configuration is displayed in sections on this page. The engine name is shown in the section title. This page shows you all Active Directory connections for all servers connected to this database. ◦ If your system was created prior to 21.2, there will be an XML section that shows Active Directory settings for pre-21.2 servers. For all systems created in 21.2 or later, those engines will use either the custom configuration defined for them, or if no custom configuration is defined, they will use the default configuration.
	Mapping Table	Allows you to see (but not edit) the mappings that exist between the Venafi Platform fields and the attribute names from the identity provider.
	Options	Driver Loading Rank allows you to specify the rank of this identity provider relative to other identity providers in the Identity Providers tree. (A lower value is a higher-priority connection.)
	Search Expressions	Search Timeout threshold Search Expression and Classes for Users, Groups, and Distribution Lists. Name Resolution Attributes

To edit an AD object using the Active Directory Identity Provider Wizard

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the Platform Connectors pane, click the Active Directory connector that requires changes.
4. (Optional) To view settings, in the **Actions** pane, under the Identity driver name, click **Properties**.



5. Click **Re-Run Wizard**.
6. Navigate the wizard and make your changes.

Viewing and changing the Active Directory connection

You can use Venafi Configuration Console to view and change Active Directory connections. If a connection requires deleting, see "Deleting an Identity connector in VCC" on page 670.

Identity Driver actions panel

Identity drivers can have the following available actions. Only the actions that apply to a specific identity driver are shown when you click on in the Platform Connectors panel.

Action	Description
Re-run wizard	Opens the same wizard you used when you created the identity driver. The wizard walks you through all configuration options one step at a time.
Enable Rediscovery	Global setting to allow rediscovery on all engines. If this setting is enabled, engine-specific discovery settings will be honored, allowing you to specify which engines can be used for rediscovery.
Disable	Global setting to disallow rediscovery on any engines.

Action	Description
Rediscovery	If this setting is enabled, no engines will run rediscovery, regardless of their individual engine settings.
Delete	Deletes this identity connector.
Properties	Opens the properties window. The specific settings you see in Properties depends on the type of identity connector you are viewing.

To view and change Active Directory connections

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the Platform Connectors pane, click the AD Identity Connector that requires changes.
4. (Optional) To view settings, in the **Actions** pane , under the Identity driver name, click **Properties**.
5. Click **Re-Run Wizard**.
6. Navigate the wizard and make your changes. For parameter descriptions and restart information, see "Creating an Active Directory connection" on page 638.

Deleting an Active Directory connection in VCC

When you delete an Active Directory connection, this is what happens in Trust Protection Platform:

- All permissions assigned to User and Group objects in the deleted directory are removed.
- All notifications resolved through contacts in the deleted directory are disabled.
- All Approval Requests assigned to User or Group objects in the deleted directory are disabled.

To delete an identity connector in VCC

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the left pane of VCC, click **Connectors**.
4. In the **Platform Connectors** pane, click the AD or LDAP Identity Connector.

5. In the **Actions** pane, click **Delete**.
6. Log in with Master Admin privileges and click **OK**.
7. Confirm.

Viewing external identities and assigning the Master Admin role

To view external Identities and assign the Master Admin role

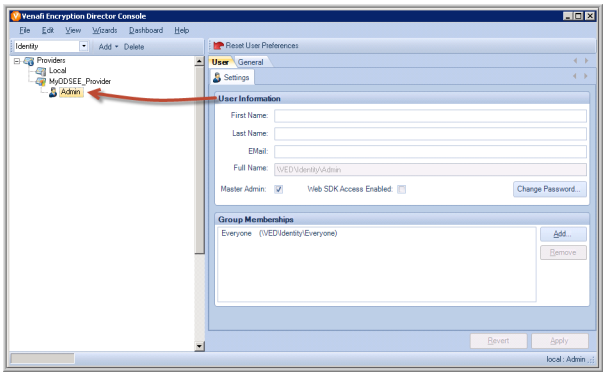
1. From the Platform menu bar, click Policy Tree while logged in with a master admin account.

   You must log in as an AD user in the current directory to view other users or groups in that AD directory. For example, if you have three AD connections, you must log in to AD1 to see its contents, AD2 to see its contents, and AD3 to view its contents.

2. Depending on your AD environment, you can log in using one of the following formats:
   - SAM account name
   - Domain name syntax (*domain_name**username*)
   - User Principle Name syntax (*valid_user*@*orgUnit.domain*.com)
3. Select the Identity tree from the Tree drop-down menu.
4. In the Identity tree, select the external user directory object.
5. On the **Identity Filter** tab, enter a search query.

   For information on narrowing the attributes and classes that Trust Protection Platform searches, see "Defining search expressions for AD user directories" on page 740.

6. Click **Apply** to retrieve the user list.
7. Select the external identity you want to view.

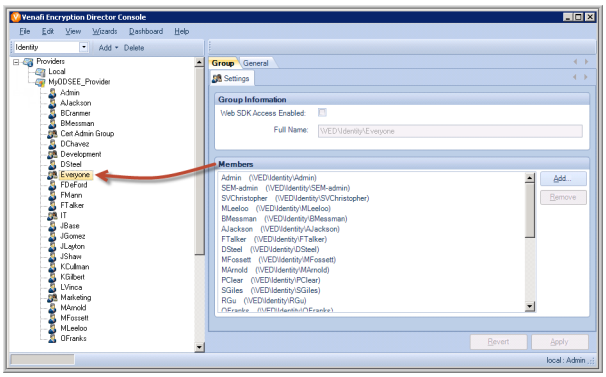


You also have the option of flagging the user or group with the Master Admin role. This role grants the user (or group members) all permissions to all objects in the Trust Protection Platform database. It is equivalent to the Local:Admin user.

WARNING! Use the Master Admin role with extreme caution. Users to whom you assign the Master Admin role have *full permissions to every object in the Trust Protection Platform database, including certificates, private keys, and credentials*. You cannot hide any objects in the system from users who have been given this role.

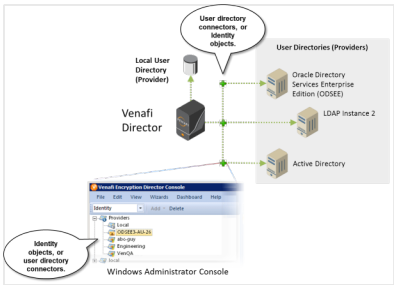
Because Trust Protection Platform uses Active Directory as a read-only user directory, the Master Administrator attribute is stored only in Trust Protection Platform.

You can view only those group members that are included in the AD Group object's Member attribute. These are also the only members that are returned in Trust Protection Platform macro results.



Working with LDAP and Oracle directory service

Venafi Trust Protection Platform™ includes Lightweight Directory Access Protocol(LDAP) support for connecting Trust Protection Platform to Oracle Directory Server Enterprise Edition, 11g for LDAP (ODSEE) (formerly, Sun® Directory Server Enterprise Edition).



Trust Protection Platform's LDAP feature is based on a standard implementation (see RFC4510). This is because each variation of LDAP includes many unique methods for accomplishing similar tasks, such as how to resolve group memberships.

Similar to Active Directory, LDAP connections are read-only. Trust Protection Platform reads user and group data directly from LDAP in real time so you can log in as an external user, view external users and groups in the Identity tree, select external users or groups as object Contacts, and assign object permissions to external users and groups.

NOTE In Trust Protection Platform, user directories are closed systems. This means that local users can see only local users and groups. Likewise, external users can see only external users and groups within their own directory (or, if enabled within their own directory and the local directory). For example, if you have three LDAP connections, you must log in to LDAP1 to see its contents, LDAP2 to see its contents, and LDAP3 to see its contents.

For information about allowing external identities to see local identities, see "Allowing AD and LDAP users to see teams and local users" on page 688.

Trust Protection Platform supports concurrent connections to multiple external user directories. This enables you to effectively distribute encryption system administration in environments that utilize multiple user directories.

Requirements for creating an LDAP Identity Provider

The LDAP Identity Provider Wizard lets you create and configure LDAP identity provider connections. Similar to the Active Directory (AD) wizard, the LDAP wizard lets you create and add a new LDAP Identity Provider object to the Identity tree.

NOTE As with the AD wizard, the LDAP wizard is only available in the Windows Administrator Console. However, you can view the settings in Policy Tree.

TIP Before running the wizard, gather the following information (if you do not already know it) so that you'll have it ready when it is required by the wizard.

For the provider to establish a connection to an LDAP server, you must provide the following information:

- **A host name or IP address of an existing LDAP server** - Specify a fully qualified DNS host name or IP address of the LDAP directory to which you want Trust Protection Platform to connect.
- **Port value** - You must be able to specify a correct port value for the LDAP Identity Provider connection. The default port value is 389.

- **LDAP authentication credentials** - Know the correct user credentials (user name and password) that can be used for LDAP authentication. This account must meet the following requirements:

  Have the required permissions to access the LDAP server that you want to include in the connection

  Be provided in DN format. For example, `cn=Administrator,cn=Users,dc=example,dc=com`

- **A name for the new LDAP identity provider** - You must specify a unique name.

About Configuring Security

During the LDAP wizard, you are required to specify an encryption method. Which one you choose depends on which method is supported by your LDAP server.

> **TIP** If your server supports encryption, you should choose an encryption option. Use **No Encryption** only as a last resort.

You must choose one of the following options:

- **SSL Encryption (LDAPS)**: If available on the LDAP host, you can select LDAPS in the Encryption drop-down list. Selecting this option changes the default port to 636.
- **No Encryption**: If available, select No Encryption for a non-SSL connection. This options sets the port to the default (389).
- **StartTLS Extension**: If available, you can select STARTTLS Encryption, which changes the default port to 636.

Creating an LDAP connection

You can use the Venafi Configuration Console to create and view LDAP connections. A connection allows Trust Protection Platform to read User and Group data directly from an LDAP Identity Provider.

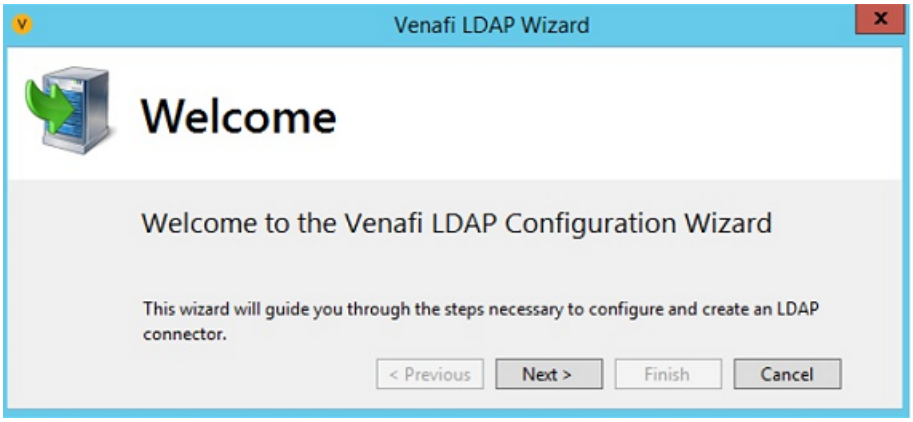
The Venafi LDAP Identity Wizard makes a connection from Trust Protection Platform to an LDAP Identity Provider. After the LDAP Identity Wizard completes, only the LDAP users and groups you specify can log in and use Trust Protection Platform based on assigned object permissions.

Trust Protection Platform supports LDAP identity object connections to providers using any of the following Internet protocols:

- IPv4 or IPv6-only connections
- IPv4 or IPv6 dual-stack (DS) connections

To create an LDAP connection

1. If you have not already done so, download and install the certificates required to establish an SSL connection with the LDAP server. If you are using the ODSEE vendor for LDAP, you can configure the LdapVendor.Oracle-DSee-11g.xml file to match your environment. For additional information about configuring for other vendors, contact Product Support.
2. Remote into the Trust Protection Platform server as a master administrator.
3. From the Windows **Start** menu, click **Venafi Configuration Console**.
4. In the left pane of VCC, click **Connectors**.
5. In the **Actions** pane, click **LDAP Connector**.
6. On the Welcome page, click **Next** and then log in with your credentials.



7. On the **Before You Begin** page, read the requirements, and then click **Next**.
8. On the **Connection Information** page, configure the connection between Trust Protection Platform and the LDAP Identity Provider, and then click **Next**.

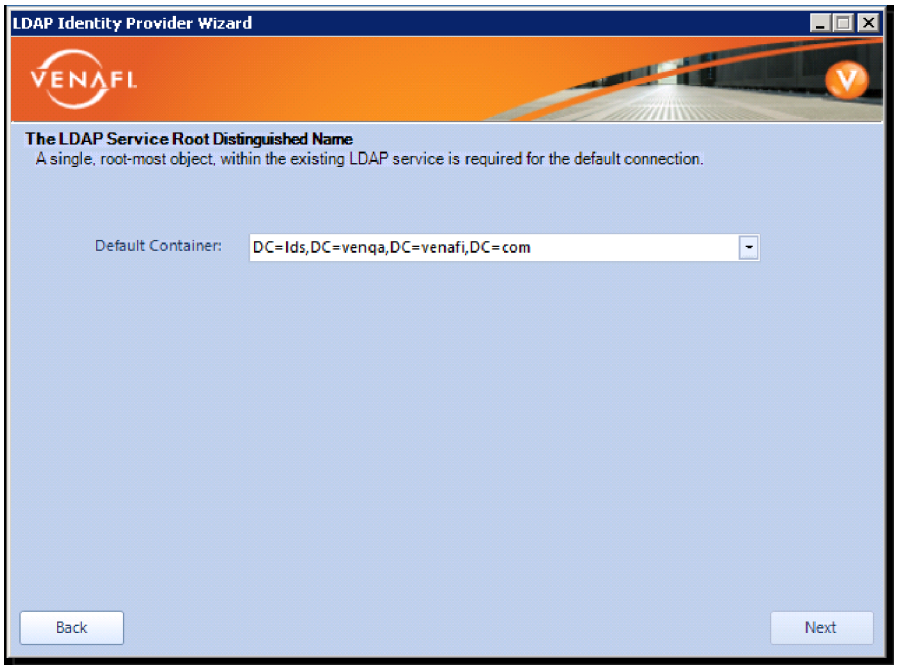
Parameter name	Description
Name / Address	A fully qualified DNS host name or IP address of the LDAP directory that requires connectivity to Trust Protection Platform.
Port	The port number for the connection between Trust Protection Platform and the LDAP Identity Provider. The default port is 636 for Lightweight

Parameter name	Description
	Directory Access Protocol over TLS/SSL.
Timeout	The maximum number of seconds to search the provider for identity information.
Encryption	The kind of encryption to use between Trust Protection Platform and the LDAP Identity Provider: ◦ **No Encryption**: No encryption. (Not recommended). ◦ **Use SSL Encryption (ldaps://)**: The encryption is LDAP over Secure Socket Layer (SSL). ◦ **Use StartTLS Extension**: The extension to serialize secure and plain requests against the LDAP server on a single connection.
Disable certificate revocation check	(Optional) Bypass checking the revocation list to determine whether the encryption certificate is revoked.
Allow anonymous binds	(Optional) Retrieve the initial binding context to the identity provider. If this option is cleared, the wizard connects via the user name and password that you supply on the next screen of the wizard. To retrieve the required naming contexts, the wizard anonymously binds *only* for the purpose of reading the rootDSE. All subsequent actions performed by the wizard will *always* perform a user bind.
Use 'Member Of' for group membership resolution	(Optional) Allow group membership resolution.
Disable user and group search validation by wizard	(Optional) Bypass validating the users and groups.

9. On the **Authentication Credentials** page, specify the required user Distinguished name (DN) and password of the Identity provider, and then click **Next**. For example, the User DN: cn=Admin,dc=odsee-qa,dc=venqa,dc=venafi,dc=com.

   > **TIP** If you get an error that an LDAP vendor cannot be determined and that there's no available map was found, see the How To: Create new LDAP vendor map for new LDAP provider KB article.

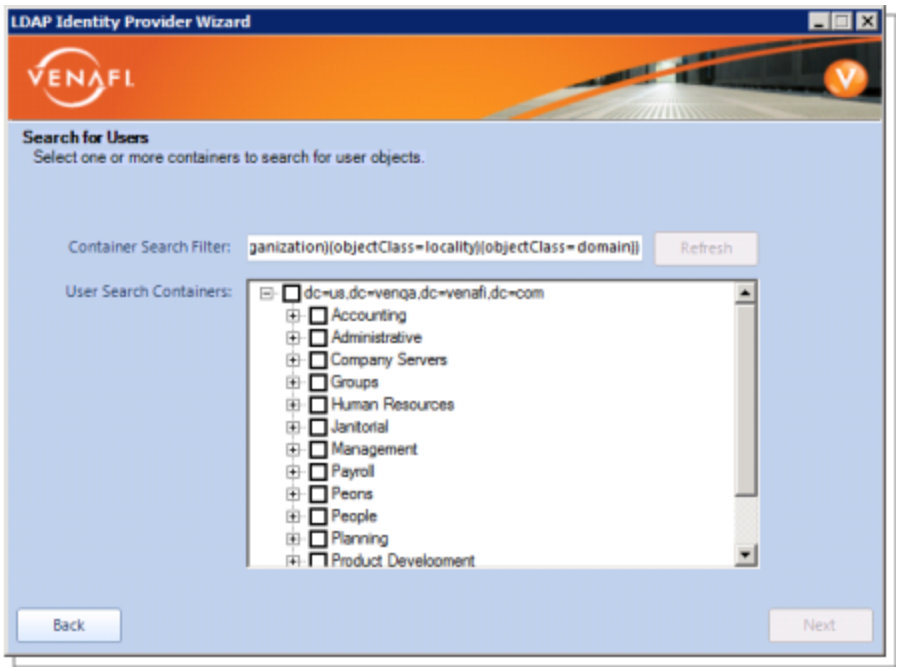
10. On the **Search Base** page, select the **Default container** from the list to search for user and group folders, and then click **Next**. No folders higher in the tree than this folder will be visible in future searches.



11. On the **User Search Root** page, type a folder search value in the **Container Search Filter** box, and then click **Refresh**. For example,
    `(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=folder))`

    The results only list the User Classes list and the Group Search Expressions that are adaptable. The Remaining fields are read-only.

12. Select the user containers to include in the search. and then click **Next**.



13. On the **Group Search Root** page, do one (or both) of the following, and then click **Next**:
    a. (Optional) if you want your selections from the previous screen to be replicated in the **Group Search Containers** tree, select **Match User Search Containers**.
    b. (Optional) In the **Group Search Containers** tree, expand and select the groups to include in the search.

       The users and groups in the folders you select will be visible in the new LDAP connection that you are creating.
14. On the **Finalization** page, specify the following values as appropriate, and then click **Next**.

Parameter name	Description
Object Name	A name for your new LDAP Identity Provider object that appears in the Identity tree and in VCC. Choose a unique name that can help your administrators more easily recognize the providers.
Friendly Name	A name for internal use by Trust Protection Platform. Type a brief name with only alphanumeric characters and spaces. The **Friendly Name** can match the **Object Name**. However, the **Friendly Name** must be unique

Parameter name	Description
	for this object type in Trust Protection Platform.
Rank	The search order for this identity provider. If there are multiple identity providers, Trust Protection Platform searches for credentials starting with the lowest number first. In the case where there are identical names, such as Administrator, Trust Protection Platform finds the first instance. If the password is incorrect, no additional searches occur in the other providers.

What's next

1. Restart the Trust Protection Platform and Venafi Log Server services as well as any Web or Policy Tree sessions.
2. (Optional) If you want to log into Policy Tree as an LDAP user, restart the IIS server that is running on your Trust Protection Platform server. You can use the iisreset command to restart the IIS server.
3. Assign groups and users who need access to the new provider.
4. To review or update basic settings from VCC, click **Properties**.

Modifying existing LDAP Identity Provider objects

You can view and edit an existing LDAP Identity Provider object in the following ways:

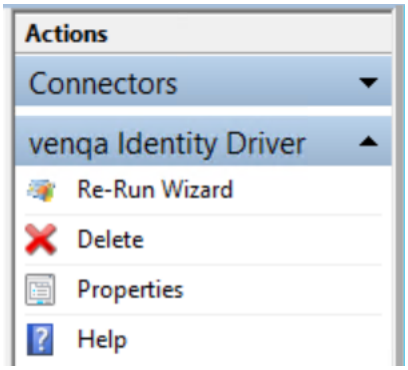
- Edit: **In the Venafi Configuration Console, run the LDAP wizard again**: Use this option if you want to change any of the settings.
- View: **In the Policy Tree, manually modify object settings**: From the Identity tree, open the **Provider** tab of the object. The following table shows you the information you can see in Policy Tree:

Tab	Sub-tab	Configuration settings
Provider		
	Settings	◦ Friendly name used to display the identity driver in the UI ◦ Hostname of the identity provider.

Tab	Sub-tab	Configuration settings
		◦ User DN. ◦ Encryption ◦ Timeout threshold ◦ Resolve Nested Groups settings ◦ Match Group Search Roots to User Search roots option ◦ Search roots for users and groups
	Mapping Table	Allows you to see (but not edit) the mappings that exist between the Venafi Platform fields and the attribute names from the identity provider.
	Options	Driver Loading Rank allows you to specify the rank of this identity provider relative to other identity providers in the Identity Providers tree. (A lower value is a higher-priority connection.)
	Search Expressions	Search timeout threshold Search expressions classes for both users and groups. Name resolution attributes

To edit an LDAP object using the LDAP Identity Provider Wizard

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the Platform Connectors pane, click the LDAP Identity Connector that requires changes.
4. (Optional) To view settings, in the **Actions** pane, under the Identity driver name, click **Properties**.



5. Do one of the following:
    - Click **Re-Run Wizard**, or
    - Click **Properties**.

If you are re-running the wizard, see "Creating an LDAP connection" on page 650 for parameter descriptions and restart information.

If you are looking at the properties window, see .

LDAP Identity Driver Properties reference

In Venafi Configuration Console you can view and edit existing LDAP driver properties.

When you open Venafi Configuration Console, browse to **Connectors**, and find your LDAP connector, then in the **Actions** panel, click **Properties**.

The following table provides a reference for the LDAP identity driver properties window.

Tab name	Field Name	Description
General	Friendly Name	(Read-only) The service provider name from the LDAP wizard. It appears as the connection label in the Identity tree and is used to reference the associated users and groups in events and internal object DNs.
General	Hostname	(Read-only) The name of the LDAP directory host, or it's virtual address.
General	User DN	(Read-only) The User Distinguished Name for the LDAP Service Account that is used to connect to LDAP and submit authentication

Tab name	Field Name	Description
		requests. This user is the current directory master LDAP Administrator.
General	Encryption	(Read-only) Shows the encryption method used to secure the connection between the LDAP connector and the LDAP server.
General	Certificates	(Read-only) Shows if the system checks for revocation of the server certificate
General	Description	A description you can use to help you identify information about this connector.
General	Password	Password to connect to the LDAP server.
General	Loading Rank	(When using multiple identity connectors). The order that Venafi Platform looks at Policy Tree user directories. Venafi Platform looks at the lowest ranked user directory first. By default, the Driver Loading Rank for all Identity connectors is zero (0). If you have multiple connections for the same provider, you must modify the Driver Loading Rank to reflect your system usage.
General	Connection Timeout	The maximum number of seconds to search the provider for identity information.
General	Search Timeout	Period of time (in seconds) that Venafi Platform waits for the external user directory to respond to its search query before it times out. In defining this value, consider the size of your directory and your system latency. Increase the value for larger directories and longer response times.
General	Resolve Nested Groups	Forces Venafi Platform to always resolve the members of nested groups for emailing notifications, approval requests, and reports. If you have multiple tiers of nested groups in your LDAP environment and you have assigned these groups as object contacts, approvers, and report recipients, it is recommended that you select this option to ensure all group members receive notifications, approval requests, and reports via email.

Tab name	Field Name	Description
General	Lockout Attribute	The attribute used to show if a user is locked out of the system. If this attribute is not set, a user locked out in LDAP may still be able perform the following operations: ■ Obtain a new OAuth token with a refresh token. ■ Authenticate to the system with SAML. ■ Authenticate to the system using a certificate. Because not all LDAP providers are universal in their implementation, you may need to either (1) manipulate your own versions of the map files; or (2) manually update this attribute name to the one used by your LDAP provider for this purpose. Lockout requires that you enable an intruder lockout policy in your LDAP server. If you create an intruder lockout policy after you have implemented Venafi Platform, you should re-run the LDAP connection wizard, or manually set this attribute. Identities are cached for 10 minutes. If a user's lockout is modified in LDAP, it may take up to 10 minutes for Venafi Platform to receive the updated information. Additionally, most LDAP systems will not clear the 'Locked Out' attribute until after a successful login after the lockout period has expired.
Attribute Matching	<Field> maps to <Field>	Allows you to map user and group field attributes from the LDAP provider to Venafi Platform fields. Venafi Platform has the following mappings for resolving user identities: ■ Give Name ■ Internet EMail Address ■ Surname ■ User Principal Name

Tab name	Field Name	Description
		■ Full Name If these attribute names do not match what is in LDAP, you can define the mappings you need.
Attribute Matching	Existing mapped attributes window	Displays the current user and group mappings.
User Search	Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. Generic uses the following search expression to narrow the search string entered on the tab to only the user class designated in the User Class Name field: `(&(|(sAMAccountName=$search$*)(cn=$search$*))(objectClass=$userclass$))` The `(cn=$search$*)` variable is the search string entered on the Users & Groups tab.
User Search	Available Classes	Classes you can select from.
User Search	User Classes	The classes you currently have selected.
Group Search	Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. Generic uses the following search expression: `(|(objectClass=groupOfNames)(objectClass=groupOfUniqueNames))`
Group Search	Available Classes	Classes you can select from.
Group Search	User Classes	The classes you currently have selected.
Login Name resolution	Available Attributes	The list of attributes you can use to resolving login names.

Tab name	Field Name	Description
Login Name Resolution	Login Name Attributes	The selected attributes you are using to resolve login names.
Search Resolution	Available Attributes	The list of attributes you can search to resolving login names.
Search Resolution	Login Name Attributes	The selected attributes you are using to resolve login names.

LDAP connection settings

The LDAP connection settings show an identity's access to Trust Protection Platform. To view LDAP users or change connection settings, you must log in as a LDAP user. For more information, see "Logging in" on page 17.

After you log in, the Identity tree, shows current values for local and directory service providers. However, you can only edit settings from the same provider that you specified during log in.

IMPORTANT After you save LDAP Identity Provider settings, you must:

- Restart the Trust Protection Platform and Venafi Log Server services.
- Reset the IIS web server of the Venafi Trust Protection Platform server.

The following table describes the configuration settings for the LDAP Identity Provider. The tab Information originates from the Active Directory (AD) Wizard.

Field	Description
Provider, Settings tab (Read Only)	Shows directory service provider information. ■ **Friendly Name**: The service provider name from the Active Directory (AD) Wizard. It appears as the connection label in the Identity tree and it is used to reference the associated users and groups in events and internal object DNs. ■ **Hostname:** The name of the LDAP directory host or virtual address. ■ **User DN**: The User Distinguished Name for the LDAP service account that is used to connect to LDAP and submit authentication requests. This user is the current directory master LDAP Administrator. ■ **Encryption**: The method to secure the connection between the LDAP connector and the LDAP server. ■ **Timeout**: The number of seconds to search before timing out. ■ **Resolve Nested Groups**: Forces Trust Protection Platform to always resolve the members of nested groups for emailing notifications, approval requests, and reports. If you have multiple tiers of nested groups in your LDAP environment and you have assigned these groups as object contacts, approvers, and report recipients, it is recommended that you select this option to ensure all group members receive notifications, approval requests, and reports via email. ■ **Match Group Search Roots to User Search Roots**: A check box that lists dc information in the User Search Roots and Group Search Roots sections. ■ **User Search Roots**: Shows or omits user search results based on the **Match Group Search Roots to User Search Roots** check box. ■ **Group Search Roots**: Shows or omits group search results based on the **Match Group Search Roots to User Search Roots** check box.

Field	Description
Provider, Mapping Table tab	Available only for AD and LDAP providerrs. Maps user and group field attributes from the LDAP/ODSEE provider to Trust Protection Platform fields. Trust Protection Platform has the following mappings for resolving user identities: Given Name, Internet EMail Address, Surname, User Principal Name and Full Name. If these attribute names do not match what is in the Identity system, you can define additional mappings in the Name Resolution section of the Provider Settings tab. For more information, see "Defining mapping rules for LDAP user and group attributes" on page 669. ■ **Field Name**: Field Name (Venafi Trust Protection Platform) ■ **Provider Attribute Name**: Provider Attribute Name (LDAP/ODSEE) ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file. ■ Refresh the data on this tab.
Provider, Options tab	Shows the order for searching LDAP user directories. ■ **Print**: Print the data on this tab. ■ Refresh the data on this tab. ■ **Driver Loading Rank**: For multiple identity connectors. The order that Trust Protection Platform looks at Policy Tree user directories. Trust Protection Platform looks at the lowest ranked user directory first. By default, the Driver Loading Rank for all Identity connectors is zero (0). If you have multiple connections for the same provide, you must modify the Driver Loading Rank to reflect your system usage.
Provider, Search Expressions tab	Provides search capability for the Users and Groups tab: ■ **Print**: Print the data on this tab. ■ Refresh the data on this tab.

Field	Description
	■ **Search Timeout**: Period of time (in seconds) that Trust Protection Platform waits for the external user directory to respond to its search query before it times out. In defining this value, consider the size of your directory and your system latency. Increase the value for larger directories and longer response times. ■ **Search Expression**: Available for Users and Groups. Provides the option of selecting a generic, predefined search expression or defining a custom search. Generic uses the following search expression to narrow the search string entered on the tab to only the user class designated in the User Class Name field: (&(|(sAMAccountName=$search$*) (cn=$search$*))(objectClass=$userclass$)). The (cn=$search$*) variable is the search string entered on the Users & Groups tab. ■ Custom allows you to modify the Expression field. You can edit the Generic search expression or enter your own. ■ **Login**: The available Ambiguous Name Resolution (ANR) attributes for searching. ■ **Search**: The available ANR attributes to use as part of the LDAP login.
Users & Groups Tab	Provides LDAP search capability for a directory service. Searches for users, groups, or both based on the Provider Search Expressions tab settings: ■ **Add**: Add an identity to the directory service. ■ **Delete**: Remove an identity from a directory service. ■ **Search**: Works in conjunction with the **Show** filter. Searches these Oracle Directory Server Enterprise Edition (ODSEE) default attributes: cn, uid, ou, o, dc, mail, givenName, or sn. By default, the search finds entries with attributes that *start with* the search string. To filter searches, use the asterisk (*) wild card in the search string. For example:

Field	Description
	◦ j: Finds all entries with attributes that start with *j*. ◦ *j: Finds all entries with attributes that have *j* anywhere within the attributes. To see details about search results, double-click the record. For more information, see "Filtering user directories in Policy Tree" on page 744. ■ **Record Limit**: The maximum number of search results. ■ **Show**: Filter Search results: **All** lists group and user identity search results together. **Users** lists only user identities. **Groups** lists only group identities. ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file. ■ Refresh the data on this tab. ■ ☐ Check box to select search results for additional actions. ■ **Name**: The search results for LDAP group or user given names. The results are based on the **Show** filter. ■ **Full Name**: The full hierarchical structure for the user or group originates from the directory service.
Users & Groups, Details User tab	Appears after you click a name from the **Users & Groups** tab. The user details that originate from the directory service: ■ **Print**: Print the data on this tab. ■ Refresh the data on this tab. ■ **Full Name**: The full hierarchical structure from the directory service. ■ **First Name**: The user's given name.

Field	Description
	■ **Last Name**: The user's last name. ■ **Email**: The user's email address. ■ **UPN**: The user's email address in the User Principal Name (UPN) format. ■ **Master Admin**: A checkbox to show whether the user has master administrator permissions. ■ **Allow Web SDK Access**: A checkbox to control whether the user can make REST API calls to Trust Protection Platform.
Users & Groups, General Entitlements tab	Available for all User and Group search results. Entitlements for the user or group that you select from the search results. The objects that the current user has been granted explicit permissions. The tab provides a convenient, centralized view of a User object's permissions assignments. In Policy Tree, the user entitlements are listed on the User Objects General tab: ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file. ■ Refresh the data on this tab. ■ **Via**: The user name. ■ **Subsystem**: The Trust Protection Platform subsystem name for which the user is entitled, for example, Config. ■ **Object**: The Subsystem object name for which the user is entitled. If the Subsystem, does not have any objects, this field is blank. ■ **Permissions**: The granted privilege, for example, AllPrivileges, Supervisor, PrivateKey, Certificate, PKCS12.
Users & Groups, Support Preferences tab	Available for all User and Group search results. Support preferences for the user or group that you select from the search results: ■ **Clear All**: Resets all user preferences.

Field	Description
	■  **Print**: Print the data on this tab. ■  Refresh the data on this tab. ■ **Subsystem**: The Trust Protection Platform subsystem name for which the user is entitled, for example, Config. ■ **Name**: The preference name. ■ **Value**: The corresponding value
Users & Groups, Group Members tab	Group member details based on the group you select from the search results. Group information originates from the directory service: ■  **Add**: Add an identity to the directory service. ■  **Delete**: Remove an identity from a directory service. ■  **Search**: The search string for retrieving users with in the group. ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file. ■  Refresh the data on this tab. ■ **Name**: The search results for LDAP group given names. ■ **Full Name**: The full hierarchical structure for the user or group from the directory service.
Users & Groups, Group Settings tab	Group access to Aperture and Web SDK based on the group you select from the search results. Shows user information from the directory service: ■  **Print**: Print the data on this tab. ■  Refresh the data on this tab.

Field	Description
	■ **Master Admin**: A checkbox to show whether the group members have master administrator permissions. ■ **Allow Aperture User Search**: A checkbox to control whether the user can search for Identity information in Aperture. ■ **Allow Web SDK Access**: A checkbox to control whether the user can make REST API calls to Trust Protection Platform.
General, Log View tab	The event information from the service provider and permissions: ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file. ■ **Up to**: Show 1,000, 5,000, 10,000, 50,000 or 100,000 log entries on this tab. ■ Refresh the data on this tab. ■ **Client Time**: The time an event occurred. ■ **Severity Event**: One of the following event severities: Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug. ■ **Description**: The corresponding event message.
General Permissions tab	The permissions to the current object and its subordinate objects. ■ **Add**: Search a user or group and add specific permissions to Trust Protection Platform. ■ **Delete**: For a user or group, remove permissions to Trust Protection Platform. ■ **Export**: Download the contents of this tab to a CSV, tab-delimited, HTML, or XML file.

Field	Description
	■ Refresh the data on this tab. ■ **Principle**: The identity name. ■ **[Permissions]**: The permissions that are granted to the Principal. For more information, see "Assigning object permissions in the Policy Tree" on page 739.
Support, Attributes tab	A set of attributes from the provider's directory service. For additional information, contact Venafi Customer Support.
Support, Permissions Analysis tab	The summary of Trust Protection Platform permissions for this identity. For additional information, contact Venafi Customer Support.
Support, Policy Attributes tab	The summary of information from the Trust Protection Platform policy tree for this identity provider. For additional information, contact Venafi Customer Support.

Defining mapping rules for LDAP user and group attributes

You can map LDAP user or group attribute names to Trust Protection Platform user or group field names.

IMPORTANT You must have *Write* permissions to the object you are modifying.

To define a new attribute mapping

1. From the Platform menu bar, click **Policy Tree**.
2. From the **Identity** tree, select the LDAP provider.
3. Click the **Provider** tab, and then click the **Mapping Table** sub-tab.
4. Click **Add**.
5. In the **Field Name**, type the Trust Protection Platform field name.
6. In the **Provider Attribute Name** field, type the corresponding LDAP user or group attribute.

Deleting an LDAP connection

You can delete LDAP connections either in Policy Tree or in the Venafi Configuration Console. For more information, see "Deleting an Identity connector in VCC" on the next page.

As with other tree objects, you can delete an existing LDAP Identity Provider object from the Identity tree.

IMPORTANT Before you delete an LDAP connection, consider the following:

- All permissions assigned to User and Group objects in the deleted directory are removed.
- All notifications resolved through contacts in the deleted directory are disabled.
- All Approval Requests assigned to User or Group objects in the deleted directory are disabled.

To delete an LDAP Identity Provider object

1. From the Platform menu bar, click **Policy Tree**.
2. In the **Tree** list, click **Identity**.
3. (Conditional) From within the Identity tree, expand the **Providers** node.
4. Select the LDAP Identity Provider object that you want to delete, and then click **Delete**.
5. If you are sure that you want to delete the object, click **Yes** to dismiss the Identity Warning and to delete the object.

Deleting an Identity connector in VCC

In the Venafi Configuration Console, you can delete AD or LDAP identity provider connections.

To delete an identity connector in VCC

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the left pane of VCC, click **Connectors**.
4. In the **Platform Connectors** pane, click the AD or LDAP Identity Connector.
5. In the **Actions** pane, click **Delete**.
6. Log in with Master Admin privileges and click **OK**.
7. Confirm.

Viewing external identities and assigning the Master Admin role

To view external Identities and assign the Master Admin role

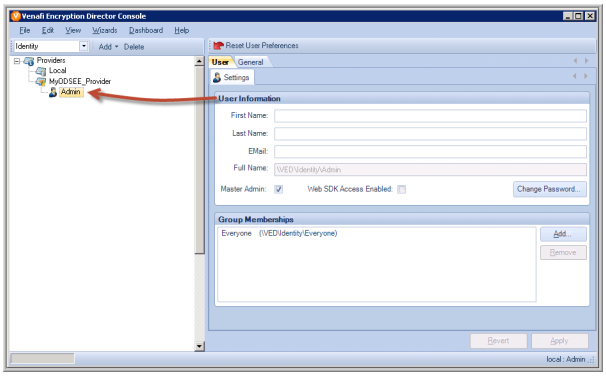
1. From the Platform menu bar, click Policy Tree while logged in with a master admin account.

   You must log in as an AD user in the current directory to view other users or groups in that AD directory. For example, if you have three AD connections, you must log in to AD1 to see its contents, AD2 to see its contents, and AD3 to view its contents.

2. Depending on your AD environment, you can log in using one of the following formats:
   - SAM account name
   - Domain name syntax (*domain_name**username*)
   - User Principle Name syntax (*valid_user*@*orgUnit.domain*.com)
3. Select the Identity tree from the Tree drop-down menu.
4. In the Identity tree, select the external user directory object.
5. On the **Identity Filter** tab, enter a search query.

   For information on narrowing the attributes and classes that Trust Protection Platform searches, see "Defining search expressions for AD user directories" on page 740.

6. Click **Apply** to retrieve the user list.
7. Select the external identity you want to view.

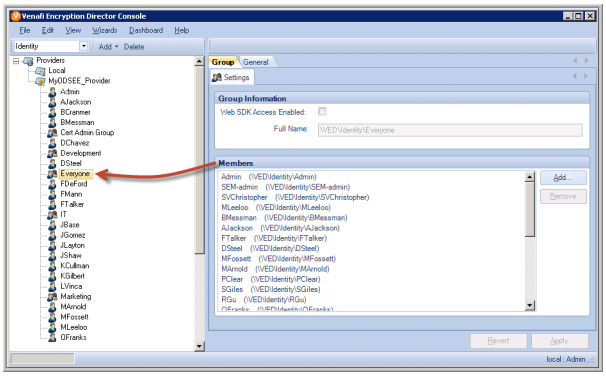


You also have the option of flagging the user or group with the Master Admin role. This role grants the user (or group members) all permissions to all objects in the Trust Protection Platform database. It is equivalent to the Local:Admin user.

WARNING! Use the Master Admin role with extreme caution. Users to whom you assign the Master Admin role have *full permissions to every object in the Trust Protection Platform database, including certificates, private keys, and credentials*. You cannot hide any objects in the system from users who have been given this role.

Because Trust Protection Platform uses Active Directory as a read-only user directory, the Master Administrator attribute is stored only in Trust Protection Platform.

You can view only those group members that are included in the AD Group object's Member attribute. These are also the only members that are returned in Trust Protection Platform macro results.



Automatic configuration of domain controllers and global catalogs

The configuration settings for domain controllers and global catalogs is simple. Trust Protection Platform actively monitors the directory connection twice daily. If Trust Protection Platform discovers any changes, it updates by adding or removing the affected domain controllers and global catalogs. No further configuration is required in Trust Protection Platform. You'll notice this when you are either configuring or updating the directory connector; the screens for domain controllers and global catalogs are still shown, but you can't make any edits to them.

Every day at noon and midnight (server time), Trust Protection Platform checks for any changes in the directory environment, and makes updates as needed. If you have made changes and want to force Trust Protection Platform to check for changes immediately, simply stop and restart the Venafi Platform service.

Allowing AD and LDAP users to see teams and local users

There's an optional setting in Trust Protection Platform that permits external identities to see local identities. This means non-admin LDAP users will be able to browse for local groups when managing contacts, identity custom fields, and when managing permissions across the product.

If you have multiple external identity providers, you don't have to enable this option for all providers. When you add identity providers to the access list, just pick the ones you want to be able to see the local identities.

To enable external users to see local identities

1. In the Policy Tree, open the **Identity** tree, and click on the **Local Identity** node.
2. On the **Provider** tab, click the **Options** sub-tab.
3. In the **Permissions** panel, click the configure button.
4. In the modal window, click the provider(s) that you want to have access to the local identities.

   > **TIP** Use CTRL + click or SHIFT + click to select multiple identities.

5. Click **Select**.
6. Click **Save**.

Creating and managing teams

Venafi Teams helps organizations streamline the process of onboarding and maintaining hundreds or thousands of teams within the Venafi Trust Protection Platform. Whether you are working with TLS certificates or SSH Keysets, its important that assets are assigned a collection of people that can share responsibility for ownership and maintenance.

Venafi Teams allows you to organize, self-manage, and automate steps within the on-boarding process so teams can start using TLS Protect and SSH Protect faster. Team owners can even manage the membership of their own teams.

Product specific team onboarding rules can be created that setup teams with the necessary folders, permissions, and policy so that teams can begin requesting and managing TLS Certificates and SSH keysets faster. See "Setting team policies and permissions" on the next page.

To enable your active directory or LDAP users to be able to see and manage teams, see "Allowing AD and LDAP users to see teams and local users" on page 688.

Setting team policies and permissions

As master administrator, you can set values such as permissions, Policy folders, and objects that teams can manage. If you want teams to manage other folders, you can change the setting in the JSON. After you save and create a team, the new folders and a team folder appear in Policy Tree. Your policy attributes appear in the team folder.

To set team policies and permissions

1. Click your **user account** icon, then click **My Teams**.
2. Click **Configure Team Settings**.
3. Do one or both:
   - If the team is for TLS Protect, customize the **TLS Protect Policies and Permissions**.
   - If the team is for SSH Protect, customize **SSH Protect Policies and Permissions**.
4. Either accept the default settings or customize the JSON. For information about the default JSON, see "Creating new folders for a team" on page 678. To customize the JSON, see "JSON recommendations for Team policy" below.
5. To apply the change to any new teams, click **Save**.
6. Create a team. For more information, see "Creating Local groups and teams" on page 702.
7. Navigate to Policy Tree and expand the Certificates or Installation folder.
8. Click the team folder and review attribute settings in their respective tab.

After you save the JSON and create a team, the new folders and a team folder appears in Policy Tree. Your policy attributes appear in the team folder.

JSON recommendations for Team policy

If you want teams to manage folders, you can change the setting in the JSON that appears on the **Team Settings**[1] page. You can also set permissions, and objects that teams can manage.

After you save, all new teams will use the updated policy. Here are some tips:

[1] To get to Team Settings, click your Uesr Account icon, then click My Teams.

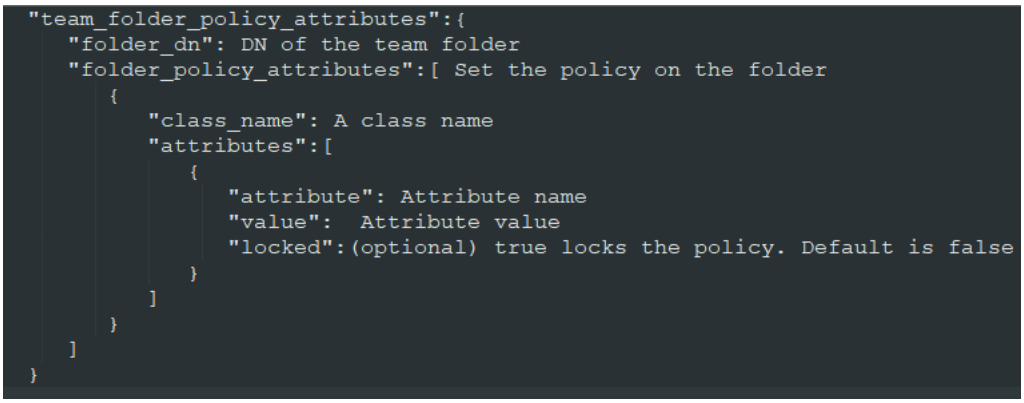
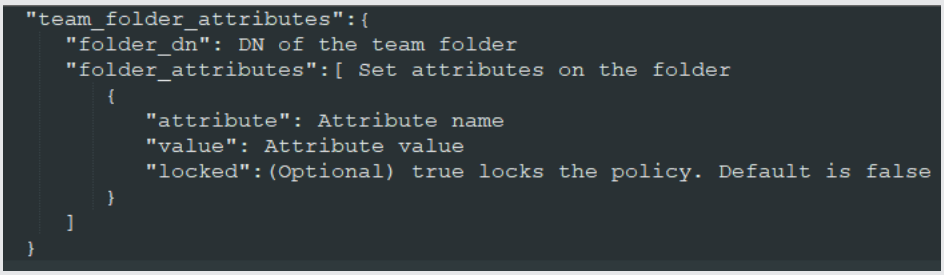
- Macro values begin and end with a dollar sign ($). The values are case sensitive. After you save, the application automatically back fills the necessary value. In the JSON, either use the default macros or type a value instead.
  - *$TeamName$*: Macro for a team name
  - *$TeamPrefixedUniversal$*: Macro for a Prefixed Universal value of a team's identity
  - *$ApplicationClasses$*: Macro for every application class
  - *$CredentialClasses$*: Macro for every credential class
- Do not change Policy attribute names. Only change the value. For example, don't change *Contacts* to a different label.



TIP To find the necessary Class names, and attributes, use a Policy Tree folder:

- **Class names and Policy attributes**: Go to the **Support Policy Attributes** tab, and click **Add**. View the names in the Class drop down. Then, locate the appropriate attribute
- **Folder attributes**: To see a list of Policy attributes, go to the Policy **Attributes** tab.

JSON object	Description
team_folders_creation	Creates team folders. Sets permissions and sets attributes on the team folders. For permissions, see "Policy Folder permissions" on page 678. For an example, see "Creating new folders for a team" on page 678. `"team_folders_creation":[{ "folder_dn": DN of the team folder "folder_permissions": Optional. A combination of permission values "folder_policy_attributes":[Optional. Set the policy on the folder { "class_name": A class name "attributes":[{ "attribute":Attribute name "value":Attribute value "locked":(Optional) true locks the policy. Default is false }] }] "folder_attributes":[Policy folder attributes { "attribute": Attribute name "value": Attribute value }] }]`
team_objects_permissions	Sets permissions to any object. For permissions, see "Policy Folder permissions" on page 678. For an example, see "Setting Team permissions on existing folders or objects" on page 686. `"team_objects_permissions":[ { "object_dn": Any Oject DN "permissions": A combination of permission values } ]`
team_folder_policy_attributes	Sets Team folder policy attributes. For an example, see "Setting Team folder policy attributes on an existing folder" on page 687.

JSON object	Description
	
team_folder_attributes	Sets Team folder attributes. For an example, see "Setting Team folder attributes on an existing folder" on page 688. 

```
"team_folder_policy_attributes":{
   "folder_dn": DN of the team folder
   "folder_policy_attributes":[ Set the policy on the folder
      {
         "class_name": A class name
         "attributes":[
            {
               "attribute": Attribute name
               "value":  Attribute value
               "locked":(optional) true locks the policy. Default is false
            }
         ]
      }
   ]
}
```

```
"team_folder_attributes":{
   "folder_dn": DN of the team folder
   "folder_attributes":[ Set attributes on the folder
      {
         "attribute": Attribute name
         "value": Attribute value
         "locked":(Optional) true locks the policy. Default is false
      }
   ]
}
```

Credential Class Names

While working with JSON for Teams, you can either specify the *$CredentialClasses$*macro or one of the following class names:

- *Amazon Credential*.
- *Certificate Credential*.
- *CyberArk Username Password Credential*.
- *Generational Credential* created by provisioning drivers to track versions of the certificate for future deletion.
- *Google Credential*.
- *Password Credential*.

- *Private Key Credential*.
- *Username Password Credential*.

Policy Folder permissions

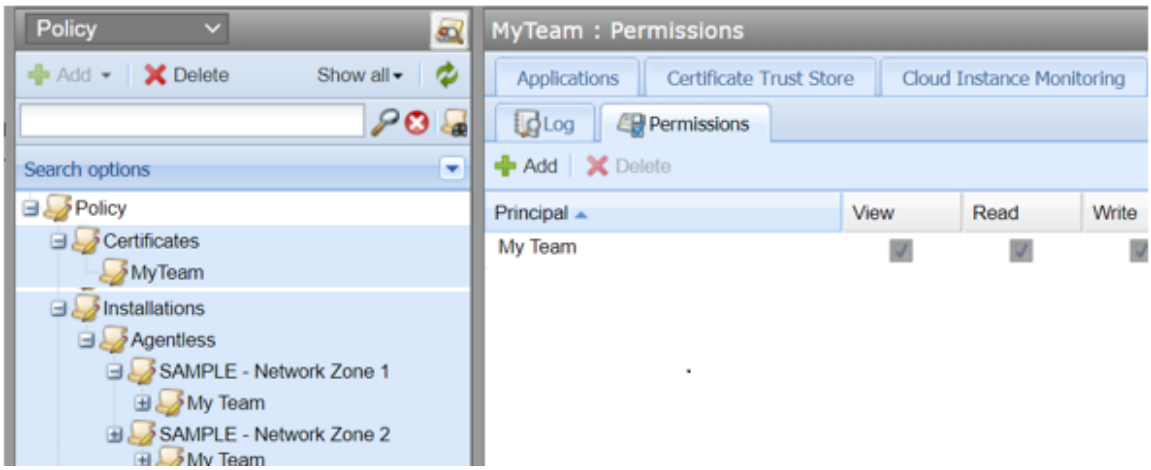
While working with JSON for Teams, you can either specify the *$CredentialClasses$*macro or one of the following class names:

- *As*: Associate
- *C*: Create
- *D*: Delete
- *Mp*: Manage Policy
- *PkR* or *PkRead* (for devices): Private Key Read
- *PkW* or *PkWrite* (for devices): Private Key Write
- *R*: Read
- *Rn*: Rename
- *Rv*: Revoke
- *W*: Write
- *V*: View

Creating new folders for a team

When you save the settings on the **Team Settings** page, the next time a new team is created, the system creates the following default folders. If you want teams to specify other folders you can update the JSON. The change applies to future team creations.

- Policy/Certificates/{team name}
- Policy/Installations/Agentless/Sample1 Network Zone 1/{team name}
- Policy/Installations/Agentless/Sample1 Network Zone 2/{team name}



To create new folders for a team

Follow the steps in "Setting team policies and permissions" on page 674. For more information, see "Policy Folder permissions" on the previous page.

Certificates folder

The example JSON:

- Creates a corresponding Team folder under the Policy\Certificates folder.
- Grants a Team permissions to the Team folder.
- Sets policy attribute settings for the Team folder.
- In the Certificate object, sets the *Contact* and *Approver* with the Team's identity.
- In the Certificate object, sets the Organizational Unit with the Team name.
- In the Device object, sets the *Contact* with the Team's identity.
- For all Application objects, sets the *Contact* and *Approver* with the Team's identity.
- For all Credential objects, sets the *Contact* will the Team's identity.
- Sets the Team folder Description attribute.

Installations folder

The example JSON:

- Creates a corresponding team folder under the Policy\installations\agent list\SAMPLE - Network Zone 1 and policy\installations\agent list\SAMPLE - Network Zone 2
- For the Device class, sets the *Contact*.
- For all Application objects set *Contact* and *Approver* with the Team's identity.
- For the Credential object, the *Contact* will include the Team's identity.
- For the Certificate object, *Contact* team *Approver* .

CA folder

The example JSON:

- Sets policy on the Administration\CAs folder to View permission. For more information, see "Policy Folder permissions" on page 678.

Example JSON

```
{
  "team_folders_creation":[
    {
      "folder_dn":"\\VED\\Policy\\Certificates\\$TeamName$",
      "folder_permissions":"V,R,W,Mp,C,Rn,As,Rv,PkR,PkW",
      "folder_policy_attributes":[
        {
          "class_name":"X509 Certificate",
          "attributes":[
            {
              "attribute":"Contact",
              "values":[
                {
                  "value":"$TeamPrefixedUniversal$"
                }
              ],
```

```
        "locked":true
      },
      {
        "attribute":"Approver",
        "values":[
          {
            "value":"$TeamPrefixedUniversal$"
          }
        ],
        "locked":true
      },
      {
        "attribute":"Organizational Unit",
        "values":[
          {
            "value":"$TeamName$"
          }
        ],
        "locked":true
      }
    ]
  },
  {
    "class_name":"Device",
    "attributes":[
      {
        "attribute":"Contact",
        "values":[
          {
            "value":"$TeamPrefixedUniversal$"
          }
        ]
      }
    ]
  },
  {
    "class_name":"$ApplicationClasses$",
    "attributes":[
      {
        "attribute":"Contact",
        "values":[
          {
            "value":"$TeamPrefixedUniversal$"
          }
        ]
```

```
        }
      ]
    },
    {
      "class_name":"$CredentialClasses$",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        }
      ]
    }
  ],
  "folder_attributes":[
    {
      "attribute":"Description",
      "values":[
        {
          "value":"Certificates for $TeamName$"
        }
      ]
    }
  ]
},
{
  "folder_dn":"\\Ved\\Policy\\Installations\\Agentless\\SAMPLE - Network Zone 1\\$TeamName$",
  "folder_permissions":"V,R,W,C,D,Rn,As",
  "folder_policy_attributes":[
    {
      "class_name":"Device",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ],
          "locked":true
        }
      ]
```

```
    },
    {
      "class_name":"$ApplicationClasses$",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        },
        {
          "attribute":"Approver",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        }
      ]
    },
    {
      "class_name":"$CredentialClasses$",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        }
      ]
    },
    {
      "class_name":"X509 Certificate",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ],
```

```
            "locked":true
          }
        ]
      }
    ],
    "folder_attributes":[
      {
        "attribute":"Description",
        "values":[
          {
            "value":"Select this folder to create installation devices that are hosted within 'SAMPLE - Network Zone
1'"
          }
        ]
      }
    ]
  },
  {
    "folder_dn":"\\Ved\\Policy\\Installations\\Agentless\\SAMPLE - Network Zone 2\\$TeamName$",
    "folder_permissions":"V,R,W,C,D,Rn,As",
    "folder_policy_attributes":[
      {
        "class_name":"Device",
        "attributes":[
          {
            "attribute":"Contact",
            "values":[
              {
                "value":"$TeamPrefixedUniversal$"
              }
            ],
            "locked":true
          }
        ]
      },
      {
        "class_name":"$ApplicationClasses$",
        "attributes":[
          {
            "attribute":"Contact",
            "values":[
              {
                "value":"$TeamPrefixedUniversal$"
              }
            ]
```

```
        },
        {
          "attribute":"Approver",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        }
      ]
    },
    {
      "class_name":"$CredentialClasses$",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ]
        }
      ]
    },
    {
      "class_name":"X509 Certificate",
      "attributes":[
        {
          "attribute":"Contact",
          "values":[
            {
              "value":"$TeamPrefixedUniversal$"
            }
          ],
          "locked":true
        }
      ]
    }
  ],
  "folder_attributes":[
    {
      "attribute":"Description",
      "values":[
        {
          "value":"Select this folder to create installation devices that are hosted within 'SAMPLE - Network Zone
```

```
2'"
            }
          ]
        }
      ]
    }
  ],
  "team_objects_permissions":[
    {
      "object_dn":"\\VED\\Policy\\Administration\\CAs",
      "permissions":"V"
    }
  ]
}
```

Setting Team permissions on existing folders or objects

The **Team Settings** page has JSON to manage existing folders and objects. The change applies to future team creations.

To set team permissions on existing folders or objects

Follow the steps in "Setting team policies and permissions" on page 674. For more information, see "Policy Folder permissions" on page 678.

Example

The following sample sets permissions on two CA templates. However, you can set Team permissions on any object. When the Team is created, Trust Protection Platform uses the Team Identity and sets the Team permissions on the CA Template.

```
{
  "team_objects_permissions":[
    {
      "object_dn":"\\VED\\Policy\\Administration\\CAs\\DigiCertStandardSSL1Year",
      "permissions":"V"
    },
    {
      "object_dn":"\\VED\\Policy\\Administration\\CAs\\DigiCert Other Cert",
      "permissions":"V"
```

```
    }
  ]
}
```

Setting Team folder policy attributes on an existing folder

The **Team Settings** page has JSON to manage existing Policy folder attributes. The change applies to future team creations.

To set policy attributes on an existing Team folder

Follow the steps in "Setting team policies and permissions" on page 674.

Example

On the Certificate object, this example sets the *Contact* with the Team Identity and *Organization* with 'Venafi, Inc'.

```
{
  "team_folder_policy_attributes":
   {
    "folder_dn":"\\VED\\Policy\\Certificates\\Internal\\$TeamName$",
    "folder_policy_attributes":[
      {
        "class_name":"X509 Certificate",
        "attributes":[
          {
            "attribute":"Contact",
            "value":"$TeamPrefixedUniversal$"
          },
          {
            "attribute":"Organization",
            "value":"Venafi, Inc",
            "locked":true
          }
        ]
      }
    ]
  }
}
```

Setting Team folder attributes on an existing folder

The **Team Settings** page has JSON to set team folder attributes. The change applies to future team creations.

To set attributes on an existing Team folder

Follow the steps in "Setting team policies and permissions" on page 674.

Example

On the Team folder, this example sets the *Description* and *Workflow* attributes.

```
{
  "team_folder_attributes":{
    "folder_dn":"\\VED\\Policy\\Certificates\\Internal\\$TeamName$",
    "folder_attributes":[
      {
        "attribute":"Description",
        "value":"Select this policy for all internal certificates",
        "locked":true
      },
      {
        "attribute":"Workflow",
        "values":[
          {
            "value":"\\VED\\Policy\\Workflows\\worflow_approval_for_csr"
          }
        ]
      }
    ]
  }
}
```

Allowing AD and LDAP users to see teams and local users

There's an optional setting in Trust Protection Platform that permits external identities to see local identities. This means non-admin LDAP users will be able to browse for local groups when managing contacts, identity custom fields, and when managing permissions across the product.

If you have multiple external identity providers, you don't have to enable this option for all providers. When you add identity providers to the access list, just pick the ones you want to be able to see the local identities.

To enable external users to see local identities

1. In the Policy Tree, open the **Identity** tree, and click on the **Local Identity** node.
2. On the **Provider** tab, click the **Options** sub-tab.
3. In the **Permissions** panel, click the configure button.
4. In the modal window, click the provider(s) that you want to have access to the local identities.

   > **TIP** Use CTRL + click or SHIFT + click to select multiple identities.

5. Click **Select**.
6. Click **Save**.

Working with teams

Identity administrators can create, edit, and delete teams. Team owners can edit teams.

To create a team

1. From your profile picture icon, click **My Teams**.
2. Click **Create Team**.
3. [Optional] Provide a team **Description**, if desired.
4. Enter the **Team Name**.
5. Select the products this team can access.
6. Add one or more Team Owners by typing the name of the identity.
7. [Optional] In the **Team Members** box, begin typing the name of an identity, then click it in the list, then repeat for as many identities you want to add to the group.
8. Click **Create**.

To review how to create teams in the Web SDK, see POST Teams.

To edit a team

After you create a team, you can modify the team settings.

> **IMPORTANT** You must have *view*, *read*, and *write* permissions on the root of the identity tree, or be a team owner to manage teams.

To edit a team in TLS Protect

1. In your user profile icon, click **My Teams**.
2. Use the filter to find the team you want to edit.
3. Click the team name in the Identity inventory.
4. On the team details page, click **Edit**.
5. Edit the team's details, including:
   a. **Team Name**. When a team is renamed, the associated folder structure also changes, if the team name only appears once in the path; however, if the path contains the team name more than once, the old team name remains. If needed, you can make the appropriate change manually.

      > **NOTE** The time it takes to rename a folder depends on the number of objects under that folder, as each item is modified separately.

   b. **Description**.
   c. **Available Products**. The products selected here will trigger the corresponding team onboarding rules defined in the JSON in the team configuration page. Making any change to the available products selected will re-run onboarding rules for all selected products.

      To update available products using the Web SDK, see PUT Teams/(prefix)/{universal}.
6. Click **OK**.

To Add People to a team

You can add team members or owners to an existing local team. When you add owners or members, those users will be added to the team and sent e-mail invitations.

NOTE The **Add People** button is not available for AD or LDAP groups, since those groups are managed in the identity provider's system. Additionally, the button does not show up for team owners, since they can edit the team directly.

Add team members

1. Click your user account icon, then click **My Teams**.
2. User the filter to find the team to which you want to add users.
3. Click the team name in the Identity inventory.
4. On the team details page, click **Add People**.
5. To add new team owners, search for the identities in the **Add Owners** box.
6. To add new team members, search for identities in the **Add Members** box.
7. Click **Save**.

When you add team members, the team owner(s) will be asked to approve the new team members. Once the membership is approved, new team members will receive a notification via email, and will being receiving relevant notifications.

If a team has no owners, master administrators will be asked to approve the membership change.

To remove people from a team

You can remove one or more people from a team using the following procedure.

1. Click your user account icon, then click **My Teams**.
2. User the filter to find the team from which you want to remove users.
3. Click the team name in the Identity inventory.
4. On the team details page, click **People**.

   The list of team members is displayed.
5. Check the box next to the members you want to remove.
6. Click the **Remove** button.

To delete a team

Deleting a team removes references to the team in the following areas:

- contacts
- approvers
- permissions
- identity custom fields

Deleting a team does *not* delete:

- certificates, devices, or keys (but it does remove the team from the contact)
- references in logs
- folders that are automatically created by the team onboarding process

IMPORTANT There is no way to undo the deletion of a team.

To delete a team

1. Click your user account icon, then click **My Teams**.
2. Use the filter to find the team you want to remove.
3. Click the team name in the Identity inventory.
4. On the team details page, click **Delete**.
5. In the modal warning box, click **Yes, Delete**.

To review how to delete a team in the Web SDK, see DELETE Teams/(prefix)/{universal}.

Join a team

It's easy to request access to join a team. When you make your request, and email is sent to the team owner for approval. When they take action, you will get an email telling you if they approved or rejected your request.

To join a team

1. First, find the team you want to join. Click your user icon, then click **My Teams**.
2. Use the **Name or Account** filter to type the first few letters of the team name. When the team name appears in the results list, click it.
3. Click **Join**.

Your request will be sent to the team owner.

> **TIP** You can see who the team owner is from the team's details screen, so you know who to contact if your request seems to be taking a while.

Team owners can view their approval requests on the Approvals screen. For more information, see "Approvals" on page 10.

Managing local identities directly in Trust Protection Platform

Like the external identity counterparts, local identities are included in a directory that is isolated from other directories containing identities from other data sources.

Even if you are using an external authentication method for the majority of your work in Trust Protection Platform, you will need to log in using your local identity to perform some system maintenance tasks including upgrading to a newer version of Trust Protection Platform.

A note about identity security across multiple directories

Groups of identities in Trust Protection Platform are maintained as closed systems called *directories*. Local users are in one directory, and each external data source is a separate directory. As a rule, users can only see other users within their own directory. (However, you can allow users in an external directory to view users in the local directory.)

This means that local users can only see local users and groups. If you have a single Active Directory connection, then when you are logged in via your AD account credentials, you can only see users and groups that are from that directory, or data source, but not any local users (unless configured) or any users from a different data source.

If you have multiple AD connections, you will only see users and groups that belong to the AD source connected to your account, as well as local users, if configured. This support for multiple external user directories enables you to effectively distribute system administration in environments that use multiple user directories without compromising the security of each directory.

For information about connecting external identities to see local identities, see "Allowing AD and LDAP users to see teams and local users" on page 688.

IMPORTANT You should not create Active Directory connections that overlap. In some cases, the provider cannot resolve the Trust Protection Platform user's permissions assignment properly. An example of overlapping connections is Active Directory connection #1 includes domain *Alpha* which has a trust relationship with domain *Bravo*, and Active Directory connection #2 includes domain *Charlie* which also has a trust relationship with domain *Bravo*.

Managing the Local user directory

The Local user directory is automatically created during installation. The Local user directory object appears in the Identity tree the first time you log in to the administration console and it includes the master administrator account, Admin.

You must use the local master administrator account (Admin) to log in to the administration console for the first time. You can then create either additional group and user Identities in the local directory or a connection to Active Directory.

NOTE In Trust Protection Platform, user directories are closed systems. This means that local users can see only local users and groups. Likewise, external users can see only external users and groups within their own directory (or, if enabled within their own directory and the local directory). For example, if you have three LDAP connections, you must log in to LDAP1 to see its contents, LDAP2 to see its contents, and LDAP3 to see its contents.

For information about allowing external identities to see local identities, see "Allowing AD and LDAP users to see teams and local users" on page 688.

Configuring the Local connection

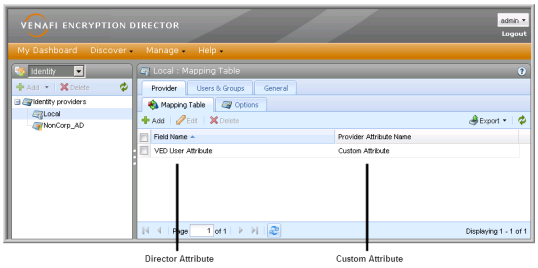
The Local Connection object is automatically created and configured during installation. It includes only two configuration options: the Permissions tab and Identity settings.

Field	Description
Users & Groups Tab	In Trust Protection Platform, user directories are closed systems. This means that local users can see only local users and groups. Likewise, external users can see only external users and groups within their own directory (or within the local directory, if configured).
 Add	Adds a user or group to the Local user directory. For more information, see "Creating local user identities" on the next page.
 Delete	Removes a user or group from the Local user directory. For more information, see "Deleting teams" on page 706.
Search	Allows you to search for a specific user or group. You can enter a combination of letters and wildcard characters to broaden the search. For example, “a*” will return all users and groups that start with the letter “a.”
Filter	Allows you to filter which objects display in the tree. The menu toggles between a Show All and Filtered state. For more information, see "Filtering the Tree view" on page 37.
 Export	Exports the data displayed on the Users & Groups tab to a CSV, tab-delimited, HTML, or XML file.
 Refresh	Refreshes the contents of the current tree.
Mapping Table Tab	
	In the Local user directory, the Mapping Table tab allows you to define the mapping rules for custom User and Group attributes that you want to reference in Trust Protection Platform macros. The Trust Protection Platform macro language allows you to call custom input for system configuration fields. This macro language is particularly useful when configuring system notifications and workflows. Using the macro language, you can call variable content for fields such as message recipient or sender, message body, or workflow approver. The default macros provided with Trust Protection Platform correctly reference local User and Group attributes. Consequently, there is no need to define mappings for the default macros. If, however, you create macros that reference attributes not defined in local User and Group objects, you must map the custom attributes to local User and Group object attributes. Mapping is required only if the attribute referenced in the macro does not match a Trust Protection Platform User or Group attribute in the local directory.

Field	Description
	For more information, see "Defining mapping rules for Local user and group attributes–Mapping Table tab" below.
Connection Settings Tab	
Driver Loading Rank	Determines the order in which Trust Protection Platform looks at the configured user directories when a user logs in to an administration console. Trust Protection Platform looks at the lowest ranked user directory first. By default, the Driver Loading Rank for all Identity connectors is zero (0). If you have multiple connections, you must modify the Driver Loading Rank to reflect your system's usage.
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Defining mapping rules for Local user and group attributes–Mapping Table tab

To define an attribute mapping for the Local Connection object, specify the Trust Protection Platform User or Group attribute under **Field Name** and the custom macro attribute under **Provider Attribute Name**, as follows:



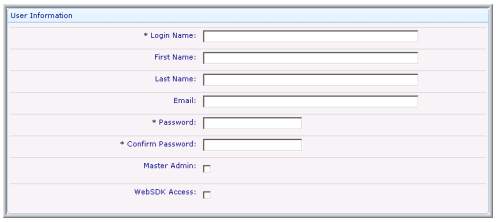
Creating local user identities

IMPORTANT You must be a Master Admin and have *Read*, *Write*, and *Create* permissions to the Local Identity object to create users and groups in the Identity tree.

To create a local user

1. From the TLS Protect menu, click **Policy Tree**.
2. Select the **Identity** tree from the tree drop-down list.
3. In the Identity tree, select the **Local** identity provider.
4. Click the **Users & Groups** tab, and then click **Add** > **User**.

   The Detail View displays the Local User object configuration settings.

5. Enter the Local user's information.

   For more information, see "Local user configuration settings" on the next page.

6. Click **Save**.

Specifying who should get default system notifications

Several object types in Trust Protection Platform let you specify user and group identities to whom you want default system notifications sent that are related to that object type. For example, you can specify contacts on policy folders, or on certificate or credential objects.

When you see a Contacts field in the Policy Tree, you can use the Identity Selector to select contacts.

To select contacts for various objects using the Policy Tree

1. Click the **Browse** button.

   The Identity Selector dialog opens.

   If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups. If you want to display all user or group entries, you can enter the wildcard character (*).

2. Select a User or Group Identity, and then click **Select**.

   Use **Shift + click** to select multiple, contiguous users and groups.

   Use **Ctrl + click** to select multiple, discontiguous users and groups.

Local user configuration settings

The following table provides a brief explanation of the User object configuration settings for creating local user accounts.

Field	Description
Login Name	Name the user will use to log in to the administration console. This is a mandatory field.
First Name	User's first name.
Last Name	User's last name.
Email	User's email address. This field is important for email notifications.

Field	Description
Password/Confirm	Password required for the user to log in to the administration console. **NOTE** Local passwords are not stored in clear text. Create a strong password by using a ■ minimum of 12 characters ■ combination of at least three of the following: ◦ one or more lowercase letters ◦ one or more uppercase letters ◦ one or more numbers ◦ one or more special characters **NOTE** You can configure password age notifications for local identities in Venafi Trust Protection Platform. For more information, see User object in the *Developer's Guide*.
Master Admin	The Master Administrator role grants the user all permissions to all objects in the Trust Protection Platform Administration Console. This role is equivalent to the Local:Admin user. You must be a Master Administrator to assign this role to other administrators. **WARNING!** Use this role with extreme caution. It gives the user full permissions to every object in the Trust Protection Platform database, including certificates, private keys, and credentials. **WARNING!** You cannot hide objects from a user with the master admin role.
Allow Web SDK Access	Gives the current administrator access to the Web SDK REST APIs. If this option is not selected, the user will not be able to log in through the Web SDK. You can disable permissions enforcement for all users who authenticate into Trust Protection Platform.

Changing local user passwords

Local users can change their own passwords the user account icon.

To change your own password

1. Click the user account icon, then click My Account.
2. Click **Change Password**.
3. Type your current password.
4. Type and confirm your new password.

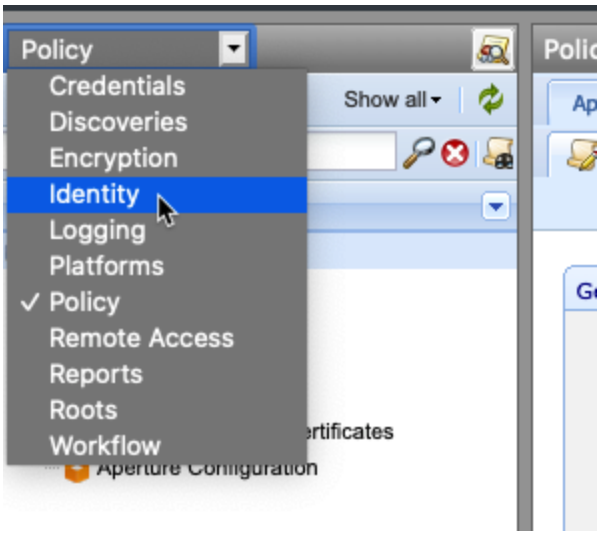
   The password complexity requirements are on the screen. As you create your password, it will be validated (client-side) to ensure it meets the complexity requirements.
5. Click **Change Password**.

Revoking a user's access grant

The following steps explain how to revoke grants issued to a specific user using the Trust Protection Platform UI. You can also revoke a user's grants using the POST vedsdk/oauth/revokegrants method.

> **NOTE** Using the UI method documented below allows you to revoke specific grants issued to the user, whereas the POST vedsdk/oauth/revokegrants method only allows you to revoke all grants issued to a user.

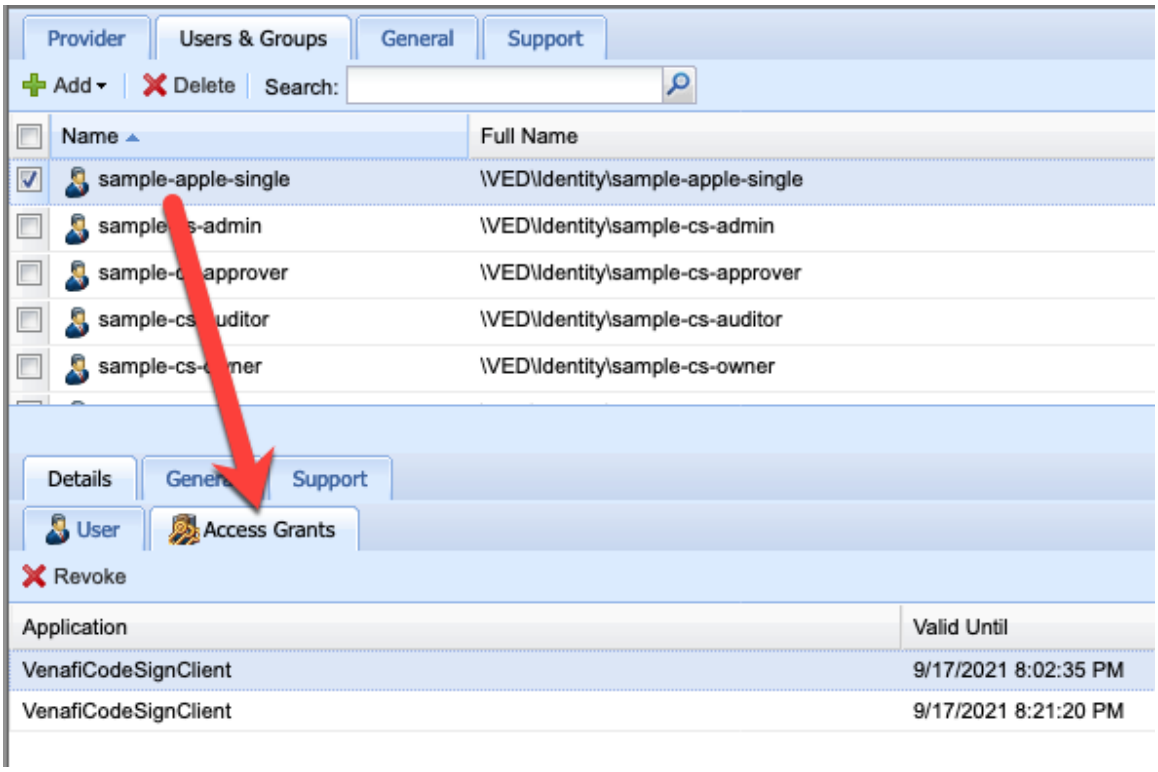
1. From the TLS Protect menu bar, click Policy Tree with either Master Admin permission or as the user that is having a grant revoked.
2. From the tree drop-down, select the **Identity** tree.



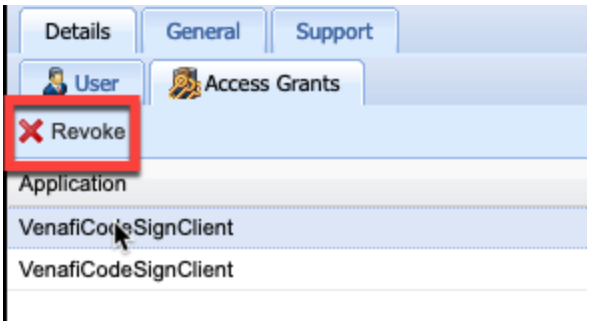
3. In the left navigation pane, select the identity provider for the user. The users for the identify provider you select will show in the main pane.
4. Select the user whose grant you want to revoke.

   NOTE Individual users can revoke their own grants, but revoking another user's grant requires Master Admin permission.

5. In the user's subtabs, click the **Access Grants** tab.



6. Click the grant you want to revoke, and then click **Revoke**.



Creating Local groups and teams

To create users and groups, you must have *Read*, *Write*, and *Create* permissions to the Local Identity object.

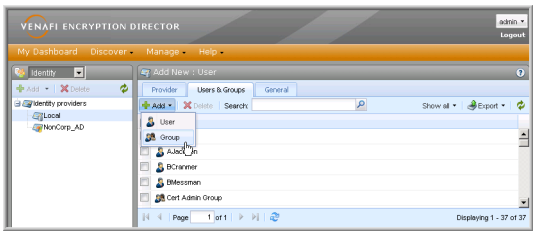
To create a team

1. From your profile picture icon, click **My Teams**.
2. Click **Create Team**.
3. [Optional] Provide a team **Description**, if desired.
4. Enter the **Team Name**.
5. Select the products this team can access.
6. Add one or more Team Owners by typing the name of the identity.
7. [Optional] In the **Team Members** box, begin typing the name of an identity, then click it in the list, then repeat for as many identities you want to add to the group.
8. Click **Create**.

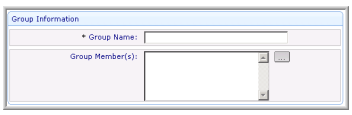
To review how to create teams in the Web SDK, see POST Teams.

To create a local group in the Policy Tree

1. From the Platform menu bar, click Policy Tree
2. Select the **Identity** tree from the Tree drop-down menu.
3. In the Identity tree, select the **Local** user directory.
4. Click the **Users & Groups** tab, and then click **Add** > **Group**.

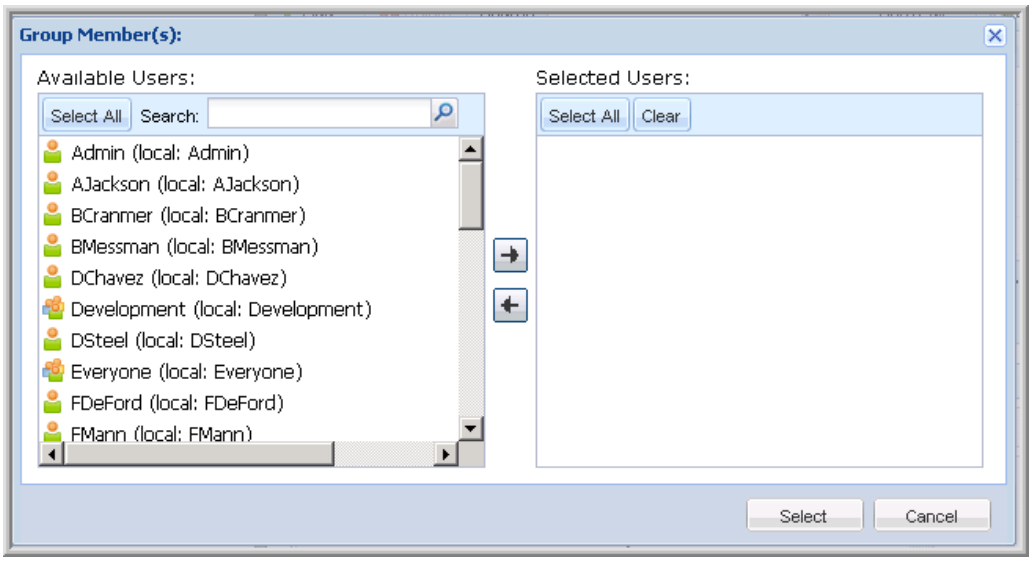


5. The **Group Information** box displays the Local Group object configuration settings.



6. Define the group name.

7. Click the **Browse** button to add group members.



8. From the **Available Users** list, select the users and groups you want to add to the current group, and then click the **Right-arrow** to move them to the **Selected Users** list.

   Press **Shift+click** to select multiple, contiguous users and groups.

   Press **Ctrl+click** to select multiple, discontiguous users and groups.

9. Click **Select** to add the members to the group.

10. Click **Save** to create the group.

About the local Everyone group

The *Everyone* group is an automated group that is created during installation. When you create users in the Local user directory, Trust Protection Platform automatically adds the users to the *Everyone* group. If you delete the *Everyone* group, Trust Protection Platform automatically re-creates it and adds all the current users in the Local user directory.

If you remove a user from the *Everyone* group, you must manually re-add the user to the group. Optionally, you can delete the *Everyone* group so that Trust Protection Platform re-creates the group and automatically re-adds all users in the Local user directory.

You do not have to manually add users to the group or continually update the group as you add new User Identities. Trust Protection Platform automatically maintains the *Everyone* group membership.

The *Everyone* group is a convenient vehicle to manage global permissions. When you assign the permissions to the *Everyone* group, those permissions are globally applied to the group's existing members as well as all new users that may be added in the future.

NOTE By default, the *Everyone* group is given the *View* and *Read* permissions.

Editing teams

After you create a team, you can modify the team settings.

IMPORTANT You must have *view*, *read*, and *write* permissions on the root of the identity tree, or be a team owner to manage teams.

To edit a team in TLS Protect

1. In your user profile icon, click **My Teams**.
2. Use the filter to find the team you want to edit.
3. Click the team name in the Identity inventory.
4. On the team details page, click **Edit**.
5. Edit the team's details, including:
    a. **Team Name**. When a team is renamed, the associated folder structure also changes, if the team name only appears once in the path; however, if the path contains the team name more than once, the old team name remains. If needed, you can make the appropriate change manually.

        NOTE The time it takes to rename a folder depends on the number of objects under that folder, as each item is modified separately.

    b. **Description**.
    c. **Available Products**. The products selected here will trigger the corresponding team onboarding rules defined in the JSON in the team configuration page. Making any change to the available products selected will re-run onboarding rules for all selected products.

        To update available products using the Web SDK, see PUT Teams/(prefix)/{universal}.
6. Click **OK**.

Deleting teams

Deleting a team removes references to the team in the following areas:

- contacts
- approvers
- permissions
- identity custom fields

Deleting a team does *not* delete:

- certificates, devices, or keys (but it does remove the team from the contact)
- references in logs
- folders that are automatically created by the team onboarding process

IMPORTANT There is no way to undo the deletion of a team.

To delete a team

1. Click your user account icon, then click **My Teams**.
2. Use the filter to find the team you want to remove.
3. Click the team name in the Identity inventory.
4. On the team details page, click **Delete**.
5. In the modal warning box, click **Yes, Delete**.

To review how to delete a team in the Web SDK, see DELETE Teams/(prefix)/{universal}.

Understanding system roles

Trust Protection Platform includes predefined system roles designed with specific permissions that you can assign to existing users.

You can see which roles are directly assigned to an identity in Venafi Configuration Console on the System Roles node. See "Managing system role assignments in Venafi Configuration Console" on page 709.

These roles include the following:

- **Access Management Admin:** grants a non-Master Admin user the permissions to modify the roles of users and groups. This role can be granted in VCC.
- **Auditor**: grants read access to view objects that are public, such as certificates, CSRs, and public keys. Also grants read access to view certain metadata about objects with higher security requirements, such as private keys. Can also read and run existing reports. This role can be granted in Policy Tree or VCC.

  > **NOTE** If the Auditor role is assigned to a user, all other permission assignments to that user are ignored.

- **CodeSign Protect Administrator:** grants a non-Master Admin full permissions to the CodeSign Protect product for creating and updating templates, flows, signing applications, etc. (This role is sometimes referred to as "Code Signing Administrator".) This role can be granted in VCC.
- **Master Admin**: grants access to every object, certificate, key, identity, and permission in the system. This role can be granted in Aperture, Policy Tree, or VCC. See "About the Master Admin role" on the next page.

  > **WARNING!** Use the Master Admin role with extreme caution. Users to whom you assign the Master Admin role have *full permissions to every object in the Trust Protection Platform database, including certificates, private keys, and credentials*. You cannot hide any objects in the system from users who have been given this role.

- **Recycle Bin Administrator**: grants a non-Master Admin user the permissions to manage the content and settings of the recycle bin. This role is particularly useful for delegating recycle bin management tasks to help desk staff without granting them full Master Admin privileges. This role can be granted in VCC.

Required access for Recycle Bin Administrator role

To use the MMC Venafi Recycle Bin Snap-In and related WebSDK APIs, the user needs to be granted access to the Venafi Recycle Bin API Integration.

To set any engine list in the recycle bin configuration, the user must also have View permissions to the root of the Platform tree.

Available actions for Recycle Bin Administrator role

A user with the Recycle Bin Administrator role can perform various actions, such as:

- Purge, restore, empty and start operations in the recycle bin.
- Configure the recycle bin settings.
- Launch the recycle bin snap-in from their desktop if they have been granted permissions to the integration.
- Perform actions using TppTool. See" Using TppTool from the command line and script files" on page 519.

How to use the Recycle Bin Administrator role

a. Open Venafi Configuration Console, click on **System Roles**.
b. Click on **Add Recycle Bin Administrator**.
c. Select a user or group to whom you want to assign the role.
d. Open either the **Access Management** MMC snap-in or go to **Aperture** > **API Integrations,** and then add the user or group to the Venafi Recycle Bin integration.
e. Ask the user to install VenafiMMC.msi on their local workstation.
f. Instruct the user to launch mmc.exe and add the '**Venafi Recycle Bin**' snap-in.
g. (Alternatively) Instead of using the snap-in, they could also use the Recycle Bin WebSDK APIs.

- **Schema Administrator**: allows non-Master Admins to modify the operational config schema of the TPP environment. This role enables delegating schema management tasks without granting full Master Admin access. This role can be granted in VCC.

  A user with the Schema Administrator role can perform the following actions:

  - Export and import TPP objects using TppTool, as long as they have permissions to the objects. See" Using TppTool from the command line and script files" on page 519.

About the Master Admin role

Trust Protection Platform includes a default administrator role called *Master Admin*. This role includes access rights to every object available in the system, including certificates, keys, identities and permissions.

When you first install Trust Protection Platform, the master admin role is assigned to the default administrator account (*admin*) by default.

You can assign the master admin role to individual users or groups. Because this role can be assigned to a group, users can be managed in this group automatically through an external identity provider, such as LDAP or Active Directory.

You can quickly see which users have the master admin role in the Identity inventory. See "Managing system role assignments in Venafi Configuration Console" below.

> **WARNING!** Use the Master Admin role with extreme caution. Users to whom you assign the Master Admin role have *full permissions to every object in the Trust Protection Platform database, including certificates, private keys, and credentials*. You cannot hide any objects in the system from users who have been given this role.

Managing system role assignments in Venafi Configuration Console

Effective management of your identities is a team effort; not one administrator needs to be in charge of everything. Venafi Platform allows you to assign system roles to specific users or groups so they can have the correct access to perform the tasks they need to do (without having to give all users access to everything).

The best way to manage system role assignments is in the Venafi Configuration Console (VCC), as described below. There is also limited ability to see some role information in the web console using the Identities inventory.

Roles can be assigned directly to a user's account, or they can be assigned to a group (either a local group, or an LDAP group). For example, suppose you have an internal help desk who is getting calls about users who accidentally delete certificates. You can add the Recycle Bin Administrator role to the LDAP group that contains all your help desk employees. Whenever a user is onboarded to the help desk team, they'll inherit this role in Venafi Platform, and when they leave the help desk team, they'll automatically lose it.

It can get complicated quickly if you are assigning roles to both individuals and groups. You may remove a role from a user account, but if the user is also part of a group with that role, the user's effective permissions would remain unchanged.

We recommend that the best practice is to assign the roles to groups, and let group management take care of permission inheritance.

For more information about roles, see "Understanding system roles" on page 706.

To add roles to users or groups using VCC

1. As a system administrator, log in to VCC using a remote session to your server, then expand the **System Roles** node.
2. In the **Actions** panel, click the **Add** button for the role you want to be added to a user or group.
3. Locate the user or group, then click the user or group name.
4. Click **Select**.

The user appears in the System Roles list with the role added. If a user has multiple roles, they will appear in the list once for each role added.

To remove roles from users or groups using VCC

1. As a system administrator, log in to VCC using a remote session to your server, then expand the **System Roles** node.
2. Locate the user or group that has the role to be removed.

   > **TIP** Set the **Group By** option to **Type** to quickly see which identities have been assigned to which roles.

3. In the **Actions** panel, click **Delete**.

About the Allow Team Creation grant

The Allow Team Creation "role" is actually a grant, not a system role. It can be seen and managed in the web console. The specific steps for adding roles and grants in Policy Tree can be found in "Managing role and grant assignments in Policy Tree" below.

Managing role and grant assignments in Policy Tree

While most system role management takes place in Venafi Configuration Console, there are a few roles you can modify directly in Trust Protection Platform's Policy Tree:

- Master Admin
- Auditor
- Allow Team Creation

> **NOTE** *Allow Team Creation* is technically a grant, not a system role, which is why it is assigned in Policy Tree rather than VCC)

To add a role/grant to a group in Policy Tree

1. From the Platform menu bar, click **Policy Tree**, then open the **Identity** tree.
2. Expand the Identity Providers group, and click the identity provider where the group is stored.
3. Make sure the **Users & Groups** tab at the top is selected.
4. Click the group identity.
5. Click the **Group** > **Settings** tab in the bottom section of the screen.
6. Select the checkbox next to the role or grant, then click **Save**.

To add a role/grant to a user in Policy Tree

1. From the Platform menu bar, click **Policy Tree**, then open the **Identity** tree.
2. Expand the Identity Providers group, and click the identity provider where the group is stored.
3. Make sure the **Users & Groups** tab at the top is selected.
4. Click on the user identity.
5. In the **Details** > **User** tab, select the checkbox next to the role or grant, then click **Save**.

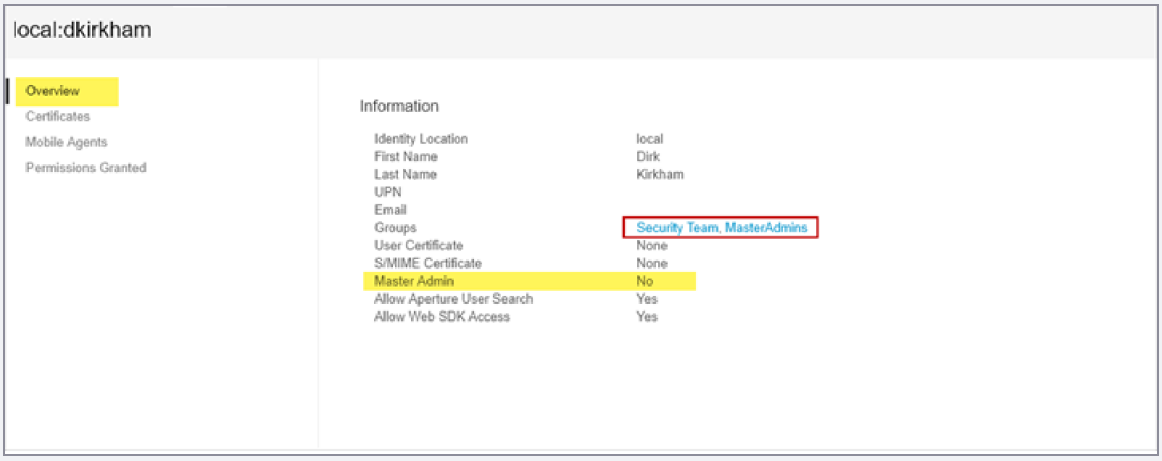
> **IMPORTANT** The checkbox is only checked if the user's identity has specifically been granted the role. Roles can be inherited via groups. In that case, the role will not be selected for the user identity, but the user will have the same access.

About viewing users that have the Master Admin role in Aperture

When viewing an identity, you can see if a user has the *master admin* role granted directly to their user object by reviewing their identity details from the Identity inventory. However, this only shows whether or not the master admin role is granted directly to the user object.

Therefore, when checking to see if a user has the master admin role from the Identity inventory, you shouldn't rely on the "Master Admin" indicator alone; you should also look at the groups to which the user is assigned so that you can verify if the groups themselves grant the master admin role.

EXAMPLE The following identity details page for a user named *dkirkham* shows that this user does not have the master admin role applied (Master Admin is set to No):



This means that the user has not been granted the master admin role directly. However, note that this user is part of two groups: *Security Team* and *MasterAdmins*. If you were to review the MasterAdmins group, you'd find that it grants master admin permissions to its members. Therefore, this user has master admin permissions to the system, even though the role has not been expressly granted to this user's account.

TIP When viewing identity details, the information shown depends on your identity and assigned roles. In the image above, Master Admin and the two additional roles below it are only visible when you're looking at your own identity, or if you had been given the master admin role directly. Non-admins cannot see this information for other users than themselves.

To learn more about roles, see "Understanding system roles" on page 706. To learn more about how to assign roles, see "Managing system role assignments in Venafi Configuration Console" on page 709.

About API Default Settings

The API Default Settings page allows you to configure access settings for token authentication, Web SDK authentication methods, and certificate authentication.

For more information, see Setting up for OAuth token authentication in the *Developer's Guide*.

Access the API Default Settings page by opening the **Platform** product, then from the menu selecting **API** > **Default Settings**.

Managing permissions for identities

The whole point of using unique users and groups is to allow you to control access to encryption objects in the system to only those users whose roles require them to have access. The information in this section will help you understand how permissions work, and how to give users access to data in the system.

For more detailed information on how permissions work across Trust Protection Platform, see "About Permissions and Inheritance" on page 716.

Permissions overview

All users listed in the Identity tree can log in to the Trust Protection Platform management console. However, what they can see and do depends upon their assigned permissions. Trust Protection Platform uses a least privileged model of system administration. So, by default, local users have only the Read permission and external users have no permissions. You must explicitly grant permissions to users before they can manage objects.

In Trust Protection Platform, all administrative permissions are managed at the object level. Every encryption system object–folders, Credentials, Workflows, CAs, Devices, Applications, Certificates, Notifications, Channels, Logging Applications, Discoveries, and Discovery Surveys–has a **permissions** tab. From the object **permissions** tab, you select the users or groups you want to have permissions to the current object and its subordinate objects, then you select which permissions you want the user or group to have.

User permissions

By default, the master administrator (created in the local user directory during installation) has all permissions to every object in the tree. For more information, see "About the Master Admin role" on page 708.

The user account used to authenticate with Active Directory also has all permissions to every object in the tree.

All other users listed in the Identity tree can log in to Trust Protection Platform from either Aperture or Policy Tree, however, what they can see and do depends upon their assigned permissions. To distribute your system's administration, the local master administrator must explicitly grant permissions to local user or group Identities. Likewise, the user account used to authenticate with Active Directory must grant permissions to external user or group Identities.

For more information, see "Assigning object permissions in the Policy Tree" on page 739.

> **NOTE** In Policy Tree, permissions assignments are updated the next time the affected user logs in to the console. The exception is when, in Policy Tree, a user has an action on the Pending Approvals page.

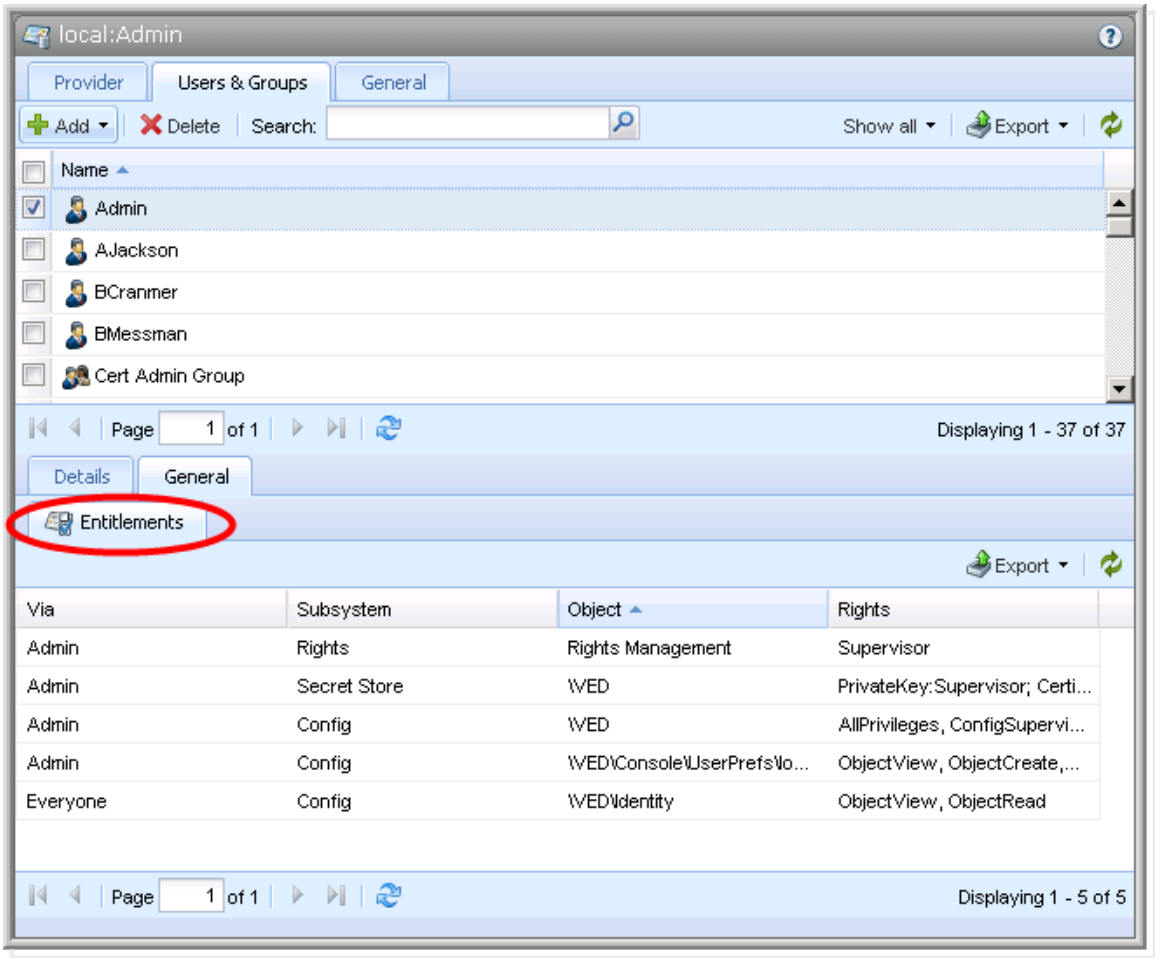
Viewing user entitlements

You can view the objects to which a user has been granted explicit permissions by viewing the Entitlements tab in a user object. This tab provides a convenient, centralized view of a user or group object's permissions assignments. Objects to which a user or group has inherited permissions do not display on the Permissions tab.

> **NOTE** Permissions assignments are updated the next time the affected user logs in.

Entitlements in the Policy Tree

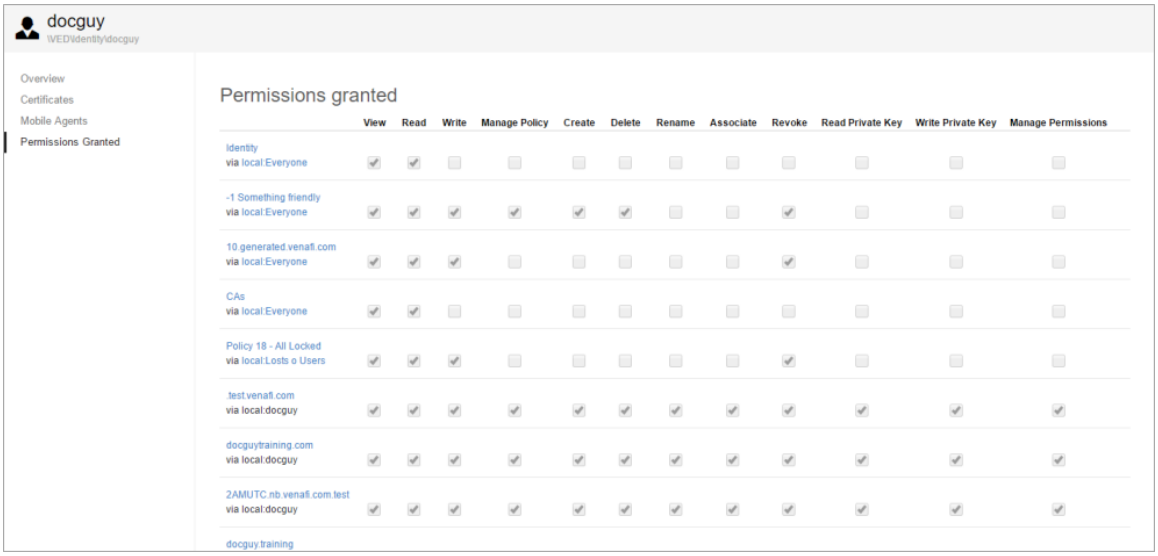
In the Policy Tree, the user entitlements are listed on a user object's General tab.



Permissions Granted

In the primary web console, user entitlements are displayed in the Permissions Granted section of the details screen for identities. The term *Permissions Granted* in the primary console is equivalent to the term *Entitlements* in the Policy Tree.

IMPORTANT You need to have Master Admin permissions in order to edit Permissions Granted.



About Permissions and Inheritance

Security of encryption assets in Trust Protection Platform is handled from a least-permissions perspective, which means that by default you have access to no assets, and you need to be granted rights to view, modify, or remove any assets. If an asset, or one of its parent objects in the folder structure (Aperture) or policy tree (Policy Tree), doesn't grant you permissions to an object, you won't be able to see that the object even exists.

The topics in this section address how permissions and inheritance work. Understanding permissions and inheritance is a key concept for understanding how Trust Protection Platform works.

This chapter contains the following topics:

Permission inheritance and flow down

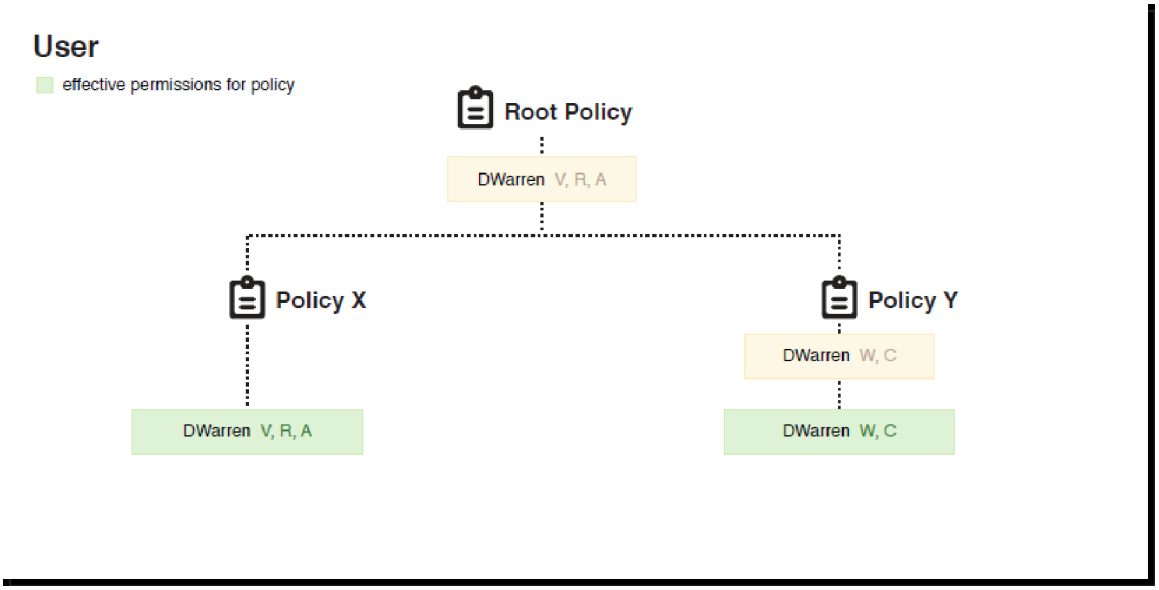
Permissions flow down the tree. This means that when you grant permissions to an object, all subordinate objects inherit those same permissions unless you explicitly grant permissions to objects further down the tree.

Therefore, permission inheritance works as follows:

- Group permissions flow down the tree to all members of the group unless overridden by User or Group permission assignments further down the tree. **Group permissions are additive.**
- **User permissions have the highest priority.** User permissions override Group permissions assigned higher in the tree, but they are added to Group permissions granted further down the tree. User permissions can be overridden only by granting different User permissions further down the tree.

User with Inherited and Reassigned Permissions

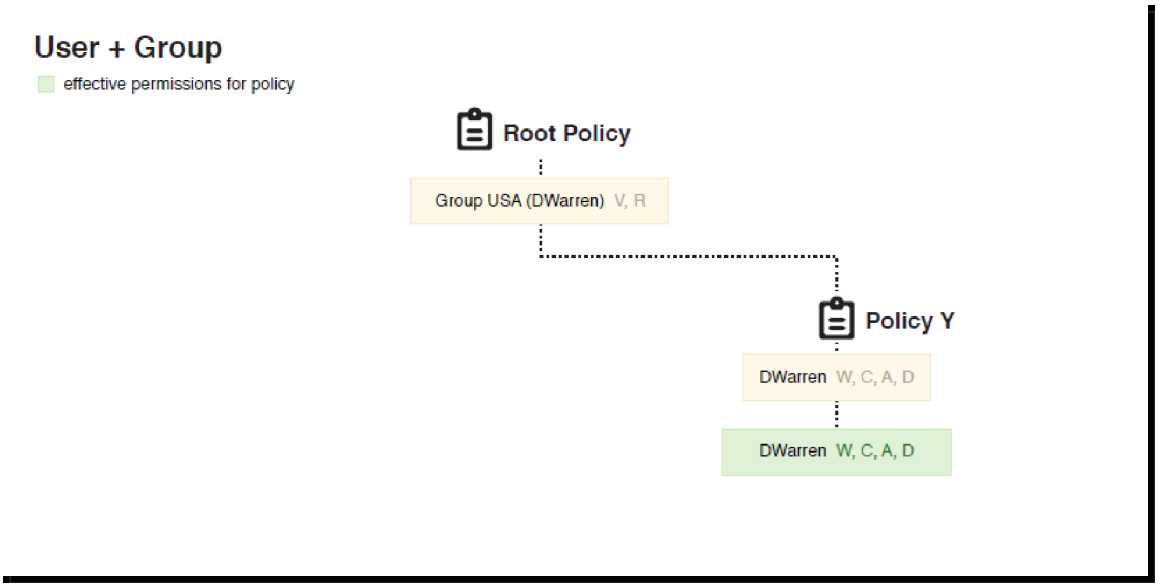
- DWarren - For Policy X, permissions of V, R, and A flow down from the Root Policy to Policy X.
- DWarren - For Policy Y, permissions were reassigned at Policy Y. Even though the Root Policy grants V, R, & A, the user permission reassignment at Policy Y overrides the Root Policy permissions.



User who is a member of a group

- DWarren - Group USA permissions at the Root Policy grants DWarren permissions V and R.
- DWarren - User permissions of W, C, A, and D are granted at Policy Y.

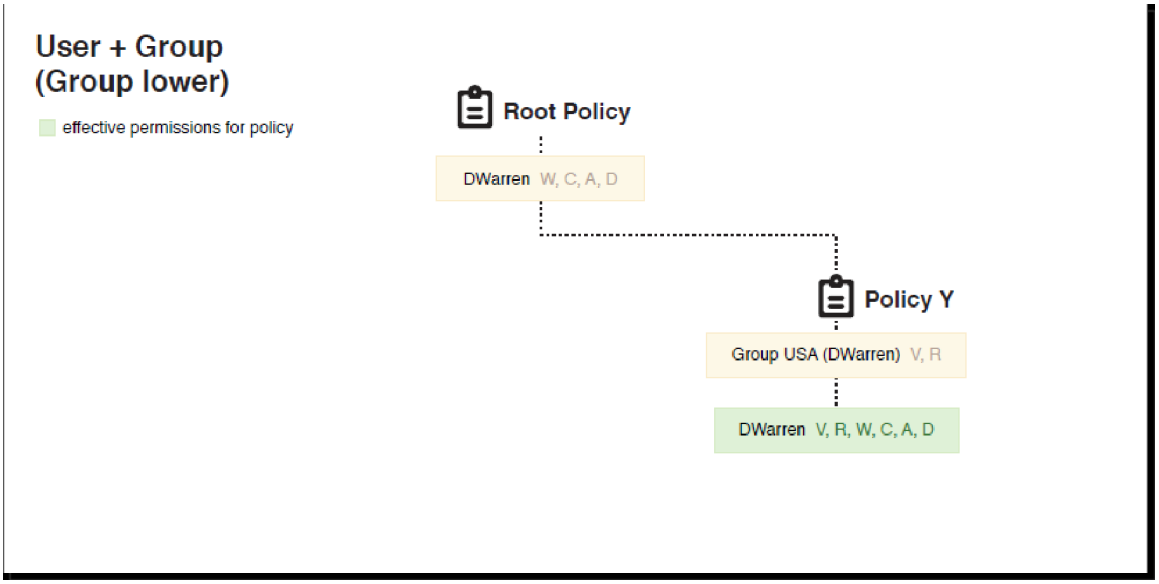
User permissions override Group permissions giving DWarren effective permission to Policy Y of W, C, A, and D.



User who is a member of a Group and the Group is lower in the tree

- DWarren - User permissions of W, C, A, and D are granted at the Root Policy
- DWarren - Group USA membership adds V and R to his permission set

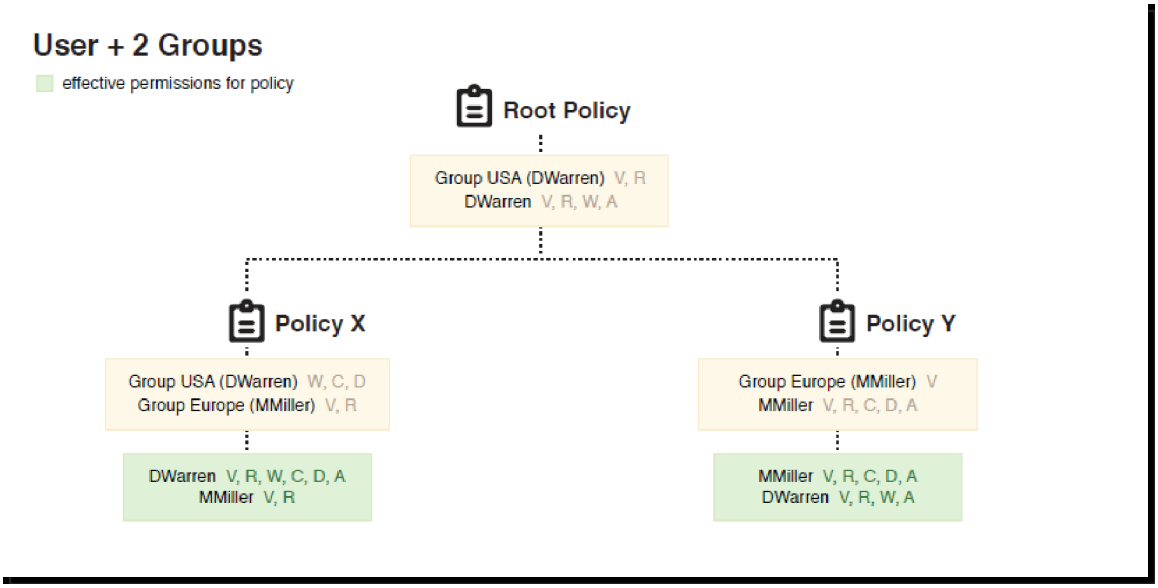
Since Group permissions are additive, DWarren's effective permissions for Policy Y are V, R, W, C, A, and D.



Two Users, each in a different Group

- DWarren has User permissions of V, R, W, and A and Group permissions of V and R at the Root Policy. Group USA gives him additional permissions of W, C, and D for Policy X. DWarren's effective permissions for Policy X are V, R, W, C, D, and A.
- MMiller has User permissions of V, R, C, D A for Policy Y. Group Europe grants him the permission of V. MMiller's effective permissions for Policy Y are V, R, C, D, and A.

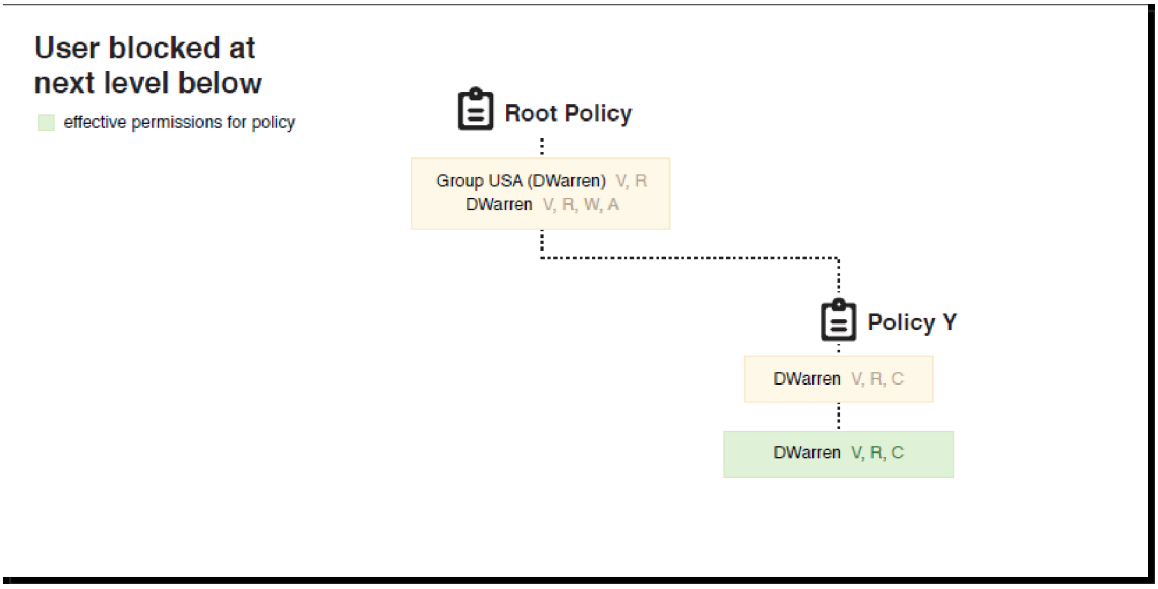
For Policy X, User and Group permissions are combined when Group permissions are further down the tree.



User blocked at the next level below

- DWarren - User permissions of V, R, W, and A are granted at the Root Policy
- DWarren - User permissions of V, R, and C are granted at Policy Y.

Since his user permissions were reassigned at Policy Y, permission A that was granted by the Root Policy is effectively blocked.



NOTE The *Create* permission implies *View*.
The *Write* permission implies *Read*.
The *Manage Policy* permission implies *Read*, *Write*, and *Revoke* but does not imply *View*. Users should be granted the *View* permission as well.

To see which permissions are assigned to a particular user or group, run an Entitlement Report. See Entitlement Report.

To learn about the Manage Policy permission, see Administrative Permissions.

About permissions

Access to items in Trust Protection Platform is controlled through permissions that are granted to individual users, or groups that users belong to.

Before you begin working in permissions, you should have a working understanding of the following:

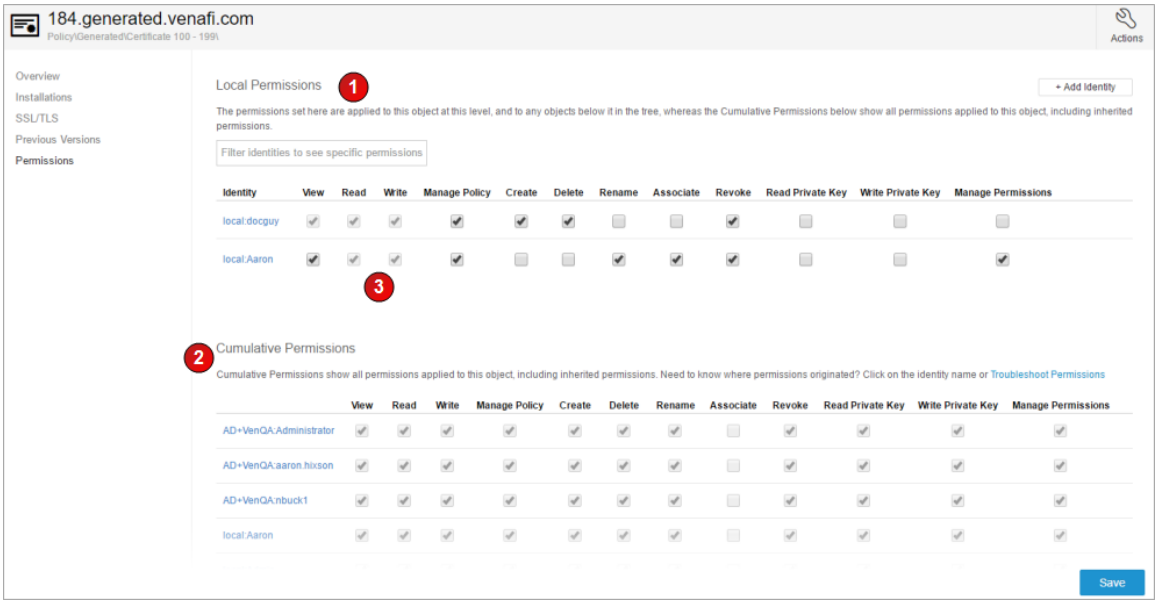
- What policies are and how the policy tree works. See About Policies.
- What permissions are and how they are assigned. See "Permissions overview" on page 713.
- How permission inheritance works in Trust Protection Platform. See "Permission inheritance and flow down" on page 717.

In Venafi Platform, permissions can be viewed for objects (certificates, keysets, devices, folders) and identities. When you are viewing object permissions, the permissions that are applied to those objects depend on where the objects are in the policy tree, because objects inherit the permissions set at the parent level (or higher) in the tree. Venafi Platform shows you both the permissions set on the current object, as well as the permissions that are effectively applied based on the object's position in the policy tree.

Permissions for objects (including certificates, keysets, folders, and devices, and jobs)

NOTE Permissions information is only available to users who have the `Manage Permissions` permission for the object they are viewing.

To view permissions for a certificate, keyset, folder, device, or job, locate the object, and then click **Permissions**.



The Permissions panel shows both local permissions (#1 in the graphic above) that are applied to this specific item (e.g. certificate or device), as well as cumulative permissions (#2) that this object inherits based on its position in the folder structure.

Permissions that are explicitly granted to this object appear as editable check boxes. Permissions that are implied based on being granted by another permission appear grayed-out, indicating they are read-only. For example, for #3 in the image above, the *Read* permission is an implied permission because of the *Write* permission that was explicitly given.

For more information about where a specific user or group was granted a permission, click Troubleshoot Permissions. For more information, see "Troubleshooting Permissions " on page 733.

Permissions for SSH keysets

In Trust Protection Platform you can manage permissions for keysets independent of the devices they are connected to. You can do this either by using policies, or through permissions set on the keyset itself.

Permissions on a keyset through policies

Keys can be moved individually, or in bulk to policy folders whereupon the applicable policy settings will be applied to the keysets. If a keyset is in a policy folder and the user has the `Manage Permissions` permission, a new tab appears on the keyset details page, allowing the user to view and edit the keyset's permissions.

When keysets are added to a policy folder, their permissions are no longer coming from the device they are connected to. Therefore, you can have a case where a user has permissions to view or edit a keyset, but doesn't have permissions to view or edit the device the keyset is linked to. In this situation, a user can still rotate the keyset, but will not be able to add keys.

Permissions on a keyset through keyset settings (for application owners)

In previous versions of SSH Protect, you had to have permissions on the device where a key was installed if you wanted to take action on the keyset. This was difficult for application owners who needed to manage keys for their application, but they didn't have admin permissions on the device.

SSH Protect now allows you to store permission information on the individual keyset, in addition to the permissions on the device object.

The table below shows what permissions are needed to take specific actions on a key or keyset, depending on whether the permissions are set at the device level **or** on the keyset. (Note in the comments when an option is provided that requires some level of permissions on *both* the device *and* the keyset.)

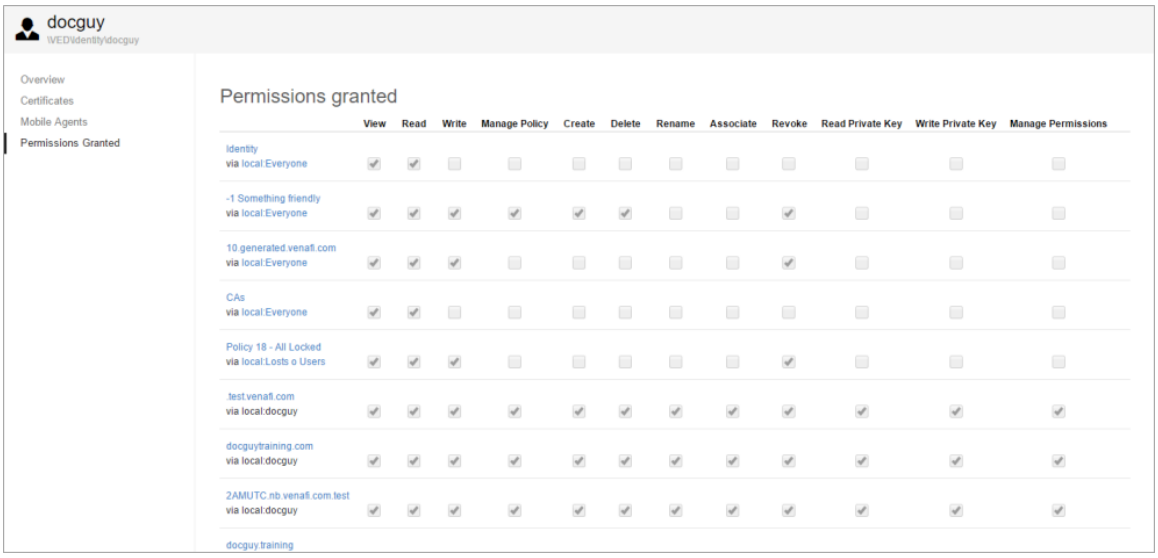
SSH Permissions required for devices vs. keysets

Action	Device	Keyset	Comments
See SSH keys	`[View & Read]`	`[View & Read]`	
Add automated private key to an existing keyset	`[View & Read & Write & Private Key Read]`	see comments	Another option is to have (on device) `[View & Create]` AND have (on keyset) `[View & Read & Write & Private Key Read]`
Add automated public key to an existing keyset	`[View & Read & Write]`	see comments	Another option is to have (on device) `[View & Create]` AND have (on keyset) `[View & Read & Write]`
Delete a key	`[Delete & Write]`	`[Delete & Write]`	Another option is to have (on device) `[View & Create]` AND have (on keyset) `[View & Read & Write & Private Key Read]`
Add or change	`[View & Read`	`[View & Read`	Another option is to have (on device)

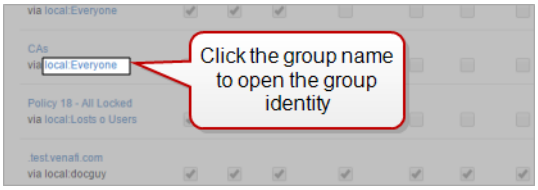
Action	Device	Keyset	Comments
passphrase of an SSH key	`& Write]`	`& Write]`	`[View & Create]` AND have (on keyset) `[View & Read & Write & Private Key Read]`
Rotate a keyset	`[View & Read & Delete]`	`[View & Read & Write]`	Another option is to have (on device) `[View & Create]` AND have (on keyset) `[View & Read & Write & Private Key Read]`
Move an existing keyset to a policy		(Source Folder: `[Delete]`) AND (Target Folder: `[View & Read & Write & Create]`)	

Permissions for identities

To view permissions for an identity, locate the object, and then click **Permissions Granted** on the left.



The Permissions Granted panel shows the object in the policy tree (policy/folder, certificate, or device) where the permission is explicitly granted. If the permission is granted to a group, you can click the name of the group to open the group identity, and see the permissions that have been granted to that group.



Object permissions

Permission	Allows the user to...
View	The user can see the object in the tree, but cannot select the object or read the values.
Read	The user can see and select the object in the tree. Additionally, the user can read the object data, but no buttons are enabled; the user cannot edit or manage the object. In Certificate objects, users with *Read* permissions to the certificate can see only the associated applications to which they have *View* or higher permissions to the Application object. In Application objects, users with *Read* permissions to the application can see only the associated certificate if they have *View* or higher permissions to the Certificate object. For SSH keysets, users with *Read* permissions to the keyset (if in a policy folder) can view all keys in the keyset. If the keyset is not in a policy folder, then the user can see all the keys in the keyset if they have *Read* permissions on all devices in the keyset.
Write	The user can edit and modify object attributes. To edit an object or its properties, you must have Write permission on the object. Note that if View permission is not granted to the device object where the application is created, the Install button will not be available for the user in Aperture. To move objects in the tree, the user must have *Write* permissions to the objects and *Create* permissions to the target folder. *Read* permissions are inferred. Rename is selected by default but can be deselected.

Permission	Allows the user to...	
	In Certificate and Application objects, the user also has access to the following options in the designated pages:	
	Certificate Summary Page	Users with *Write* permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.
	Certificate Settings Page	Users with *Write* permissions to the Certificate object have access to the Renew Now option.
	Certificate Associations Page	Users with *Write* permissions to the Certificate object can see all associated applications, regardless of their permissions to the individual applications. Users with *Write* permissions to the Certificate object can add associations only to those applications to which they have either *Write*, or both *Associate* and *View* permissions. Users with *Write* permissions to the Certificate object have access to the Retry Installation option only for those applications to which they have either *Write* or both *Associate* and *View* permissions. Users with *Write* permissions to the Certificate object can push the certificate and private key only to those applications to which they have either *Write* or both *Associate* and *View* permissions.

Permission	Allows the user to...	
		Users with *Write* permissions to the Certificate object can enable or disable the certificate only on those applications to which they have either *Write* or both *Associate* and *View* permissions.
	Application Settings Page	Users with *Write* permissions to the Application object can add associations only if no certificate is currently associated with the Application object or if they have either *Write* or both *Associate* and *View* permissions to the associated Certificate object. Users with *Write* permissions to the Application object have access to the Retry Installation option only if they have either *Write* or *Associate* and *View* permissions to the associated Certificate object. Users with *Write* permissions to the Application object can push the certificate and private key to the application only if they have either *Write* or *Associate* and *View* permissions to the associated Certificate object.
	For SSH keys, users with *Write* permissions to a keyset can rotate keys, delete keys from a keyset, add a new key, and can add a passphrase to a key. However, if the user doesn't have *Write* permissions to write to the key's associated device, then the user cannot add keys.	
Create	The user can create subordinate objects, such as devices and applications. *View* is inferred.	

Permission	Allows the user to...
	For SSH keys, you must have the *Create* permission in the target folder to move a keyset into that folder.
Manage Policy	Lets users modify policy values on folders. *Read* and *Write* permissions are implied; the *View* permission is not. In order for the Manage Policy permission to be useful, users should be granted the *View* permission, as well. For SSH keys, you must have the Manage Policy permission in the target folder to move a keyset into that folder.
Delete	Lets the user delete objects. For SSH keys, you need to have the *Delete* permission to remove keysets from all folders (returning the keyset to device-level permissions). For SSH keys, you need the *Delete* permission in the source folder when moving a keyset from one folder to another.
Rename	Lets the user rename objects or move them within the tree. To move an object, the holder must have the *Create* permission in the target location. When an object is moved, locked policy attributes are recalculated.
Associate	If you have *Write* permissions to a Certificate object and both *Associate* and *View* permissions to the application(s) where the certificate is installed, you can perform the following functions in the Certificate object's Certificate Associations page: ■ Associate or disassociate the application with the certificate ■ Push the certificate and private key to that application ■ Retry the certificate installation ■ Enable or disable the processing of certificates on the application. When you disable processing, Trust Protection Platform does not attempt to install,

Permission	Allows the user to...
	renew, process, or validate certificates for the current application. If you have *Write* permissions to an Application object and *Associate* and *View* permissions to the certificate installed on the application, you can perform the following functions in the Application object's Settings page: ■ Associate or disassociate the certificate with the application ■ Push the certificate and private key to that application ■ Retry the certificate installation This permission is relevant only to Policy, Application and Certificate objects. To associate an object with another object, you must have View permission on both objects. Additionally, to push a certificate to an installation, a user must also have View permissions to the device object where the application is created. Note that if View permission is not granted to the device object where the application is created, the Install button will not be available for the user in Aperture.
Revoke	Revoking a certificate makes it invalid. You must have *Write* permissions to the certificate. Once you Revoke a certificate, you cannot undo the action.
Private Key Read	You can download the private key from the Trust Protection Platform database, if the key is archived in the Trust Protection Platform database. This permission is relevant only to Policy and Certificate objects.

Permission	Allows the user to...
Private Key Write	You can upload a certificate private key file to the Trust Protection Platform database. This permission is relevant only to Policy, Certificate, and Private Key Credential objects.
Admin (Policy Tree only)	Grant other user or group Identities permissions to the current object or subordinate objects. In the Aperture console, this permission is called *Manage Permissions*.
Manage Permissions (Aperture console only)	Grant other user or group Identities permissions to the current object or subordinate objects. In Policy Tree, this permission is called *Admin*.

Assigning permissions to objects

Permissions for an object (certificate, device, folder, credential, or identity) can be viewed and updated easily. Venafi Platform provides all the information that is available for these objects plus it shows the cumulative permissions that are applied based on other permissions granted further up the folder structure.

To assign local permissions to a folder

1. From the TLS Protect menu bar, click **Configuration** > **Folders**.
2. Navigate the folder structure by clicking the folder icon to expand the folder, and then click the folder name you want to edit.
3. Click the **Permissions** link on the left.
4. If the identity already exists in the **Local Permissions** section, add or remove permissions by selecting or deselecting the appropriate check boxes.
5. If the identity doesn't exist in the **Local Permissions** section, do the following:
    a. Click **Add Identity**.
    b. In the **Identity** field, search for the identity that you want to the Local Permissions for this object.

c. Select the permissions that you want to add for this identity.

d. Click **OK** to close the window and preview your changes on the main permissions screen.

6. Click the **Save** button at the bottom of the screen.

> **IMPORTANT** If you don't click **Save**, these settings will not be saved, including any identities you've added to **Local Permissions**.

Reviewing permissions and assigning permissions to a non-folder item

To review effective permissions to a certificate, device, credential, or a folder

1. In TLS Protect, open the certificate, device, credential, or folder whose effective permissions you want to review.
2. Click the **Permissions** link on the left.
3. Review the identities and the permissions that are granted to an identity at either the local level, or permissions that are granted to the object cumulatively.

   For a given identity, a permission is granted to that identity if a check appears in the box for either the local or the cumulative permission.
4. To review the permissions for a specific identity or group of identities, enter the identity (or part of the identity) in the identity filter, then press **Enter**.

   If you have a large number of identities in the list, you can easily filter the list of identities to find a specific user or group by adding multiple identities to the filter. When multiple identities are in the filter, they are treated as an implied OR search, so you will see results that match *any* identity, not only results that match *all* included identities.

To review permissions for a specific identity

1. On the TLS Protect menu bar, click **Inventory** > **Identities**.
2. Use the filters on the left to search for a name or account. Click on the identity name you want to edit.

   > **TIP** The **Name or Account** filter lets you enter the name of a user or a group to review the settings for that individual or group. The **Groups** filter lets you enter the name of a group, and see all the users that are part of that group.
3. Click the **Permissions Granted** link on the left.

4. Review the objects where this identity (or a group this identity belongs to) has been granted explicit permissions to an object.

   IMPORTANT You need to have Master Admin permissions in order to edit Permissions Granted.

For more information on identity permissions, see "Managing permissions for identities" on page 713.

Assigning local permissions to certificates or devices

The recommended best practice is that you assign permissions to the folders that contain the certificate and devices, rather than explicitly assigning permissions to certificates and devices. This makes permissions management easier and more scalable for the system administrators. However, TLS Protect does allow you to assign local permissions to a specific certificate or device. If you need to assign permissions directly to these items, use the following steps.

To assign local permissions to a certificate or device

1. From the TLS Protect menu bar, click **Inventory** > **Certificates**or **Inventory** > **Devices**.
2. Locate the certificate or the device, using a filter if necessary, and click the name of the object to open the object details screen.
3. Click the **Permissions** link on the left.
4. If the identity already exists in the **Local Permissions** section, add or remove permissions by selecting or clearing the appropriate check boxes.
5. If the identity doesn't exist in the **Local Permissions** section, do the following:
   a. Click **Add Identity**.
   b. In the **Identity** field, search for the identity that you want to the Local Permissions for this object.
   c. Select the permissions that you want to add for this identity.
   d. Click OK to close the window and preview your changes on the main permissions screen.
6. Click the **Save** button at the bottom of the screen.

   IMPORTANT If you don't click **Save**, these settings will not be saved, including any identities you've added to **Local Permissions**.

Troubleshooting Permissions

Because of the flexibility of being able to assign permissions at any point in the folder structure, it can sometimes be difficult to understand why one user has permissions to an object while another user doesn't have the same permissions to the object.

Venafi Platform provides the ability to view and compare permissions between users for a given object, allowing you to see where in the folder structure one user is given permissions to an object where another user might not be. This feature is called "Troubleshoot Permissions." This feature is available to master administrators, as well as users with the *manage permissions* right.

> **NOTE** Remember, your ability to search user accounts is limited to the accounts in your own identity provider (also called a *directory*).

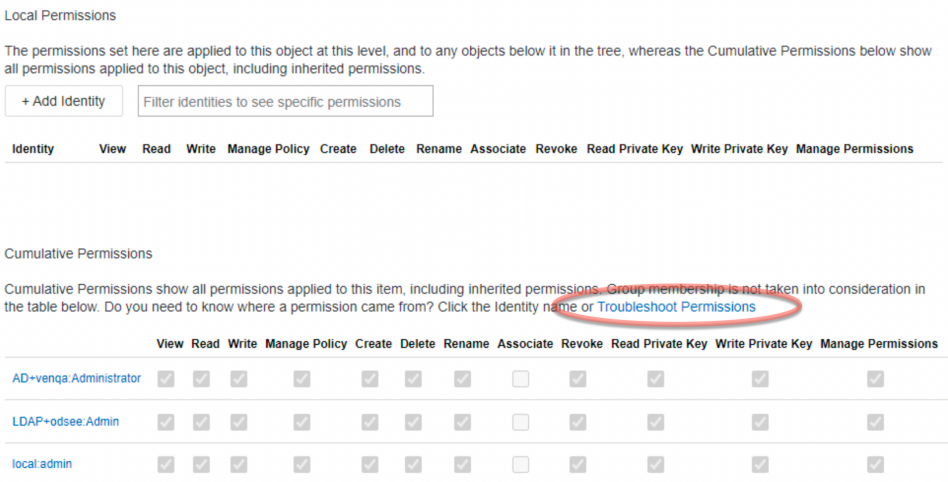
To troubleshoot permissions

1. Open the object details page, and click **Permissions** in the sidebar.

   The top group, Local Permissions, shows the permissions that have been set on the object at this level, not any inherited permissions.

2. In the **Cumulative Permissions** paragraph text, click **Troubleshoot Permissions**.

   The bottom group, Cumulative Permissions, shows all permissions that apply to this object, both those set locally, above, as well as all inherited permissions.



   The Troubleshoot Permissions window opens.

3. Enter the identity (or identities) you want to review or compare.

For each identity, you see the effective permissions granted to that identity at any level of the folder structure. If an identity has permissions granted in multiple places in the folder structure, you see the individual entries, followed by a summary of all permissions they have to the object. If you have the *manage permissions* privilege for an object or identity, you can click its name to see permissions information.

You cannot edit the permissions in this view. This view simply shows you where in the folder structure permissions have been added or removed.

> **NOTE** You can also view permissions for policy objects by clicking **Configuration** in the TLS Protect menu bar, and then clicking **Folders**. Locate the policy folder you want to edit, and open it, and then click **Permissions**.

Configuring permissions for groups and work

Trust Protection Platform lets you control who has access to view and configure the groups and work that you create.

To configure permissions for groups

1. From the TLS Protect menu bar, click **Clients** > **Client Group Settings**, and then select a group name.
2. Click **Permissions** and specify the permissions for the current group.
3. Click **Save**.

To configure permissions for work

1. From the TLS Protect menu bar, click **Clients** > **Client Group Settings**, and then select a group name.
2. In the **Work** list, click the name of the work item (in the Name column) for which you want to configure permissions.
3. On the Work page, click **Permissions**.
4. Specify local or cumulative permissions for the work.
5. When you're finished, click **Save**.

Assigning permissions to an object in Policy Tree

The **Permissions** tab allows you to assign access permissions to the current object. You can also manage permissions via parent objects, including folder.

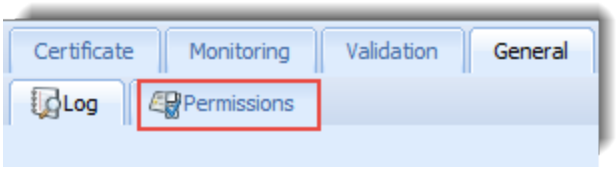
TIP Because permissions assigned in parent objects flow down the tree to the subordinate objects, defining admin permissions in a parent object, such as a Policy object, is an efficient way to manage administrative permissions to your encryption resources. It is not necessary to assign permissions to individual objects unless you want to override the permissions inherited from the parent object.

For more information on permissions management in Trust Protection Platform, see "Working with identities, permissions, and teams" on page 635 in the *Venafi Trust Protection Platform Administration Guide*. For information on assigning permissions in folder, see "Using policies to manage encryption assets" on page 859 in the *Venafi Trust Protection Platform Administration Guide*.

IMPORTANT You must have the *View*, *Admin*, and *Write* permissions to assign object permissions.

To assign permissions to an object

1. From the TLS Protect menu bar, click Policy Tree.
2. Select the **Policy** tree from the Tree drop-down menu.
3. In the Policy tree, select the Certificate object.
4. Click the **General** > **Permissions** tab.



5. Click **Add**.

   If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, enter the wildcard character (*).

6. Select a User or Group Identity.

   Press **Shift+click** to select multiple, contiguous users and groups.

   Press **Ctrl+click** to select multiple, discontiguous users and groups.

7. In the Policy Tree, click to move the users to the Selected list, and then click **Select** to add the users to the object's Permissions tab.
8. Select the permissions you want the User or Group Identity to have, and then click **Apply/Save**.

   In the Policy Tree, permissions assignments are updated the next time the affected user logs in to the console or when the user clicks Refresh in a grid or tree view.

Object permissions

The following table provides an explanation of the available permissions:

Permission	Allows the holder to...	
View	The user can see the object in the tree, but cannot select the object or read the values.	
Read	The user can see and select the object in the tree. Additionally, the user can read the object data, but no buttons are enabled; the user cannot edit or manage the object. View permissions are inferred. In Certificate objects, users with Read permissions to the certificate can see only the associated applications to which they have View or higher permissions to the Application object. In Application objects, users with Read permissions to the application can see only the associated certificate if they have View or higher permissions to the Certificate object.	
Write	The user can edit and modify object attributes. To move objects in the tree, the user must have Write permissions to the objects and Create permissions to the target folder. View and Read permissions are inferred. In Certificate and Application objects, the user also has access to the following options in the designated pages:	
	Certificate Summary Page	Users with Write permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.
	Certificate Settings Page	Users with Write permissions to the Certificate object have access to the Renew Now option.

Permission	Allows the holder to...	
	Certificate Associations Page	Users with Write permissions to the Certificate object can see all associated applications, regardless of their permissions to the individual applications. Users with Write permissions to the Certificate object can add associations only those applications to which they have either Write or Associate and View permissions. Users with Write permissions to the Certificate object have access to the Retry Installation option only for those applications to which they have either Write or Associate and View permissions. Users with Write permissions to the Certificate object can push the certificate and private key only to those applications to which they have either Write or Associate and View permissions. Users with Write permissions to the Certificate object can enable or disable the certificate only on those applications to which they have either Write or Associate and View permissions.
	Application Settings Page	Users with Write permissions to the Application object can add associations only if no certificate is currently associated with the Application object or if they have either Write or Associate and View permissions to the associated Certificate object. Users with Write permissions to the Application object have access to the Retry Installation option only if they have either Write or Associate and View permissions to the associated Certificate object. Users with Write permissions to the Application object can push the certificate and private key to the application only if they have either Write or Associate and View permissions to the associated Certificate object.
Create	Create subordinate objects.	

Permission	Allows the holder to...
	View is inferred.
Delete	Delete the object.
Rename	Rename the object or move it within the tree. To move an object, the holder must have the Create permission in the target location. When an object is moved, locked policy attributes are recalculated.
Associate	If you have Write permissions to a Certificate object and both Associate and Read permissions to the application(s) where the certificate is installed, you can perform the following functions in the Certificate object's Certificate Associations page: ■ Associate the application with the certificate ■ Push the certificate and private key to that application ■ Retry the certificate installation ■ Enable or disable the processing of certificates on the application. When you disable processing, Trust Protection Platform does not attempt to install, renew, process, or validate certificates for the current application. If you have Write permissions to an Application object and Associate permissions to the certificate installed on the application, you can perform the following functions in the Application object's Settings page: ■ Associate the certificate with the application ■ Push the certificate and private key to that application ■ Retry the certificate installation This permission is relevant only to Policy, Application and Certificate objects.

Permission	Allows the holder to...
Private Key Read	You can download the private key from the Trust Protection Platform database, if the key is archived in the Trust Protection Platform database. This permission is relevant only to Policy and Certificate objects.
Private Key Write	You can upload a certificate private key file to the Trust Protection Platform database. This permission is relevant only to Policy, Certificate, and Private Key Credential objects.
Admin	Grant other user or group Identities permissions to the current object or subordinate objects.

Assigning object permissions in the Policy Tree

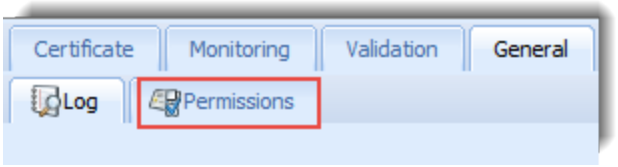
In Trust Protection Platform, all administrative permissions are managed at the object level. Every encryption system object–folders, Credentials, Workflows, CAs, Devices, Applications, Certificates, Notifications, Channels, Logging Applications, Discoveries, and Discovery Surveys–has a **Permissions** tab. From an object's **Permissions** tab, you select the users or groups to whom you want to give permissions to the current object (and its subordinate objects). And then you select which permissions you want those users or groups to have. Because permissions flow down the tree, assigned permissions are also inherited by subordinate objects.

To assign permissions to an object i the Policy Tree

1. From the Platform menu bar, click Policy Tree.

   IMPORTANT You must have the *View* and *Admin* permissions to assign object permissions.

2. Select the object you want to grant permissions to.
3. Click the **General** > **Permissions** tab.



4. Click **Add**.

If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. Because some external directories are very large and may take a long time to load, the Trust Protection Platform Administration console do not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external user directory and return the list of requested users or groups.

5. Select a User or Group Identity, and then click **Select**.

   Press **Shift+click** to select multiple, contiguous users and groups.

   Press **Ctrl+click** to select multiple, discontiguous users and groups.

6. Select the permissions you want the User or Group Identity to have, and then click **Apply/Save**.

   NOTE Permissions assignments are updated the next time the affected user logs in. The exception is in Policy Tree on the Pending Approvals pages.

For information on viewing permissions in the Aperture console see "About permissions" on page 721.

Filtering identities

If you have a large number of users or teams in your user directories, you can manage the number of identities that display in a directory or you can filter the directory.

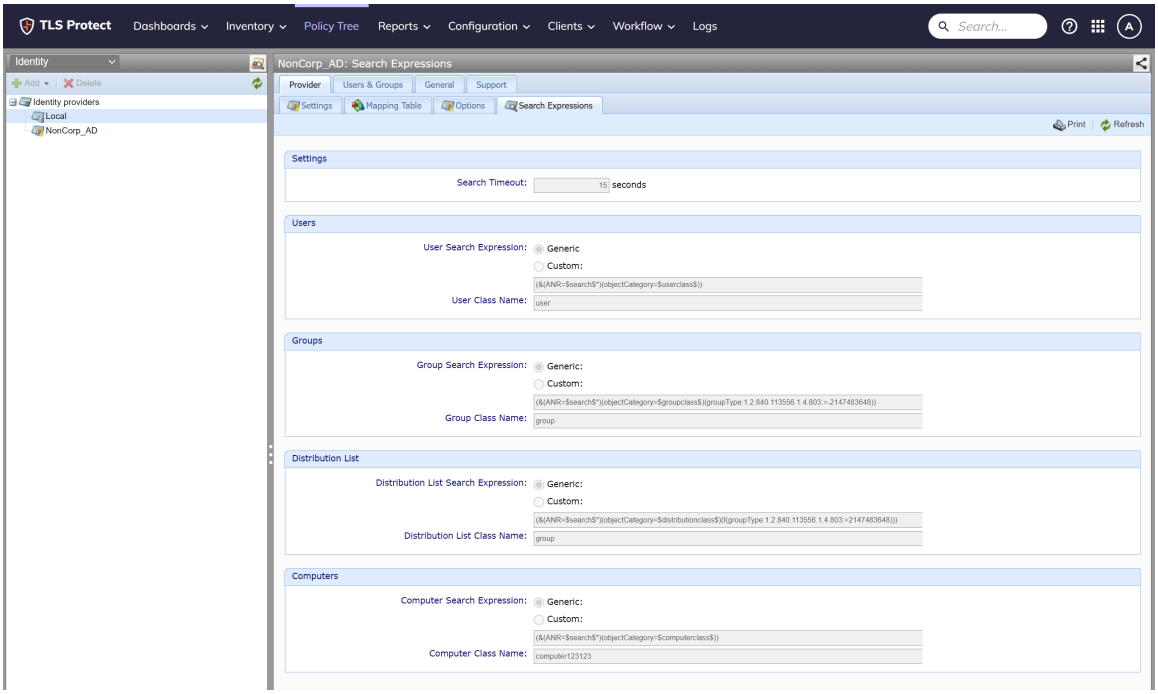
The topics in this section show how you can use identity filtering options in both Aperture and Policy Tree.

Defining search expressions for AD user directories

Because some AD user directories are very large and may take a long time to load, Policy Trees do not automatically display external users and groups. You must first type a search string so Trust Protection Platform can query the external user directory and return the list of requested users or groups.

By default, Trust Protection Platform searches all object attributes and classes for the designated search string. For large directories, this may pose significant overhead for the query. To narrow the object attributes and classes that are searched during a query, you can define LDAP search expressions on the AD connection object's Search Expression tab, which limit the search to specific user and group classes.

NOTE The WebAdmin page displays information as view only. To modify AD search expressions, use Venafi Configuration Console. Go to the Properties section of the connector.



Search Expressions Options

Field	Description
General	
Search Timeout	Period of time (in seconds) that Trust Protection Platform waits for the external user directory to respond to its search query before it times out.
Users	
User Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. ■ Generic uses the following search expression to narrow the search string entered on the Users & Groups tab to only the user class designated in the User Class Name field: `(&(|(sAMAccountName=$search$*)(cn=$search$*))(objectClass=$userclass$))`

Field	Description
	The (cn=$search$*)variable is the search string entered in the Users & Groups tab. ■ Custom allows you to modify the Expression field. You can edit the Generic search expression or enter your own as properties of the AD connector by using Venafi Configuration Console.
Expression	Search expression used to narrow the attributes and classes that Trust Protection Platform searches. Select Custom to edit this field.
User Class Name	Name of the user class that the search expression is applied to.
Groups	
Group Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. ■ Generic uses the following search expression to narrow the search string entered on the Users & Groups tab to only the group class designated in the Group Class Name field: (&(|(sAMAccountName=$search$*)(cn=$search$*))(objectClass=$groupclass$)) The (cn=$search$*)variable is the search string entered on the Users & Groups tab. ■ Custom allows you to modify the Expression field. You can edit the Generic search expression or enter your own as properties of the AD connector by using Venafi Configuration Console.
Expression	Search expression used to narrow the attributes and classes that Trust Protection Platform searches. Select Custom to edit this field.

Field	Description
Group Class Name	Name of the group class that the search expression is applied to.
Distribution List	
Distribution List Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. ■ Generic uses the following search expression to narrow the search string entered on the Distribution List tab to only the Distribution List class designated in the Distribution List Class Name field: `(&(ANR=$search$*)(objectCategory=$distributionclass$)(!(groupType:1.2.840.113556.1.4.803=2147483648)))` The `(cn=$search$*)`variable is the search string entered on the Distribution List tab. ■ Custom allows you to modify the Expression field. You can edit the Generic search expression or enter your own as properties of the AD connector by using Venafi Configuration Console.
Expression	Search expression used to narrow the attributes and classes that Trust Protection Platform searches. Select Custom to edit this field.
Distribution List Class Name	Name of the distribution list class that the search expression is applied to.
Computers	
Computer Search Expression	Provides the option of selecting a generic, predefined search expression or defining a custom search. ■ Generic uses the following search expression to narrow the search string entered on the Computers tab to only the Computer class designated in the Computer Class Name field:

Field	Description
	(&(ANR=$search$*)(objectCategory=$computerclass$)) The (cn=$search$*)variable is the search string entered on the Computers tab. ■ Custom allows you to modify the Expression field. You can edit the Generic search expression or enter your own as properties of the AD connector by using Venafi Configuration Console.
Expression	Search expression used to narrow the attributes and classes that Trust Protection Platform searches. Select Custom to edit this field.
Computer List Class Name	Name of the computer class that the search expression is applied to.

Filtering user directories in Policy Tree

Because some external directories are very large and may take a long time to load, the policy tree does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external user directory and return the list of requested users or groups.

You must have the *view* and *read* permissions to the selected directory.

> **NOTE** For information on narrowing the attributes and classes that Trust Protection Platform searches, see "Defining search expressions for AD user directories" on page 740.

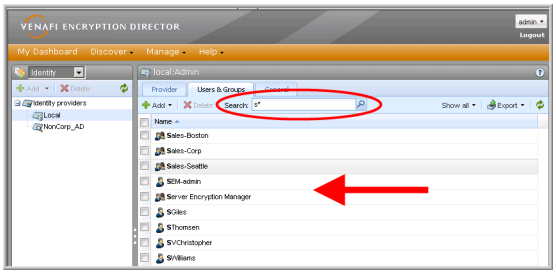
To filter a directory's users and groups in Venafi Platform

1. From the TLS Protect menu, click **Configuration** > **Classic Policy Tree**.
2. From the Tree drop-down menu, select the **Identity** tree.
3. In the Identity tree, select the user directory you want to filter. You can select the Local or an external user directory.
4. To filter the user list, click the **Users & Groups** tab.

5. In the **Search** field, type the letters you want to use as the filter, and then click the **Search** icon .

   Trust Protection Platform filters the users or groups listed in the current tab by the designated letters.

   You can also type an attribute value (attribute=value). For example, if you type “sn=smith” in the **Users & Groups** tab’s Search field, the console returns all users with a last name of “Smith”.



Modifying TLS Protect user and group permissions

TLS Protect provides the ability to give different permissions to various users or teams. For example, you can give permissions to specific identities to allow them to search, view and manage other user's certificates. This is useful when you want to delegate management tasks to other administrators.

> **BEST PRACTICE** Enable this Identity permission only for users that need to view and manage other user's certificates. User A, when given the *user search* right, will be able to see User B's certificates (but only those for which they both have the same permissions). User A can see certificates owned and managed by User B. User A can interact only with the certificates to which he and User B have the same permissions.
>
> *User search* is useful for closing potential security gaps when an employee transfers to another role or department, or leaves the company. It's critical to know which certificates were managed by that employee and take action on them.

To view an identity's permissions

1. Click your user account icon, then click **My Teams**.
2. Use the filters to locate the user or team.
3. Click on the identity name in the results list.

The permissions are listed in the information on the identity details screen.

To modify an identity's permissions

1. From the TLS Protect menu bar, click **Policy Tree**.
2. In the **Identity** tree, navigate to the provider that contains the identity you want to modify.

   > **TIP** Venafi Platform teams are always stored in the **Local** identity provider.

3. If necessary, browse to the **Users & Groups** tab.
4. Click the identity you want to modify.
5. [Conditional] If you are modifying an individual user, on the **Details** > **User** tab, modify the permissions as needed.
6. [Conditional] If you are modifying a team, on the **Group** > **Settings** tab, modify the permissions as needed.
7. Click **Save**.

Filtering by users, teams, or roles using the Identity Inventory

TLS Protect allows you to view information about users and teams that have access to objects in Trust Protection Platform. Collectively when we refer to users and teams, we call them *identities*.

Everyone can search for users or teams. However to search for roles (or to see roles on a different identity's details page, you need to meet the following condition:

- Your user account has *View* and *Read* permissions to `\VED\Identity` in the policy tree

To find a specific user, team, or role

1. Click your user icon, then click **My Teams**.
2. Do one of the following:
   a. To find a specific identity (user, account, or team) start typing the first few letters of the identity's name or account name in the **Name or Account** box.
   b. To find members of a team, start typing the first few letters of the team name in the **Membership by Team** box, then click it to see a list of its members in results panel.

c. [Conditional: If you have permissions] To find users assigned a the Master Admin role, click the **Roles** box and select **Master Admin**.

   For additional information, see "Understanding system roles" on page 706.

d. To see a single identity's groups and their roles in those groups, type the identity name in the **Members** box.

e. To see what groups a team belongs to, type the group name in the **Members** box.

Viewing identity details

An identity's details page shows you information about a specific user or team. From the **My Teams** menu, you find a user or team using filtering, and then click the one you want to view (see "Filtering by users, teams, or roles using the Identity Inventory" on the previous page).

User details

Under **Information**, you can see role information about the identity. If your account has the `Master Admin` permission, you will also be able to see some of the roles the user has.

The above settings are `read-only` on the My Account page. To modify them,

1. From the Platform menu bar, click **Policy Tree**.
2. Open the **Identity** tree.
3. Click on the identity, make changes, and save your changes.

In the side navigation you can view:

- **Certificates** – lists the certificates issued to the user and gives details about the name, expiration date, the key strength, and status of the certificate. Using the drop-down menu, you can choose to either download or revoke the certificate.
- **Mobile Agents**– lists all of the mobile agents on which the user certificates are installed. This list can include devices that were used in the past by the user. The Agent's most recent check in time is also displayed.
- **Permissions Granted**– shows all the permissions that are granted to this user, or to a group that the user is part of. If your account has a role that allows you to manage permissions for an object, click the name of the object to view the object's permissions management page. (You won't see this if you don't have the `Master Admin` role.)

Team/Group details

When you open a team or group's details page, you can see information about the team's source and permissions, as well as a list of the its members. Click a member's name to go to that user's overview page.

In the sidebar you can view the People who are part of the team. You can see their friendly name, role, unique id, the date they were added, and the name of the person who added them to the team. If you select one or more rows, you can remove those members from the team.

In the sidebar you can also view the **Permissions Granted** to the group. If your account has a role that allows you to manage permissions for the object, you can click the name of the object to view the object's permissions management page.

Updating an identity provider connection password

When an identity provider password changes, you need to synchronize the service account password in the identity provider connection. Instead of rerunning the wizard, you can use either in the Venafi Configuration Console, or with the TppConfiguration utility. The utility runs from the command line or from a script.

You can only update the service account password in Trust Protection Platform to match the password in AD or LDAP. To change or rotate the identity provider password:

- Make the change on the appropriate system.
- Use VCC to provide the service account with the updated password.

To use VCC to update the service account password

1. Remote into the Trust Protection Platform server as a master administrator.
2. From the Windows **Start** menu, click **Venafi Configuration Console**.
3. In the left pane, click **Connectors**.
4. In the **Platform Connectors** pane, click the Identity Connector that requires changes.
5. In the **Actions** pane, click **Properties**.
6. Log in with your Trust Protection Platform local, master administrator credentials.
7. On the **General tab,** type the identity provider password in **Password** box.
8. Click **Apply**, and then restart all Venafi services.

To use the command line to update the service account password

1. Remote into the Trust Protection Platform server as a master administrator.
2. From an administrative command line, navigate to *[Venafi installation folder]\Platform*.
3. (Optional) For TppConfiguration help such as syntax or return codes, type *TppConfiguration -help*.
4. Type *TppConfiguration.exe -driverpwd* and follow the prompts:

Input value	Description
Local TPP master admin name	The Trust Protection Platform local, master administrator account name.
Password	The Trust Protection Platform local, master administrator password.
Identity driver name	The common name of the identity driver.
New password for the driver	The new service account password.

For example:

```
>C:\Program Files\Venafi\Platform>TppConfiguration.exe -driverpwd
Please enter local TPP master admin name: admin
Please enter the password 'admin': ************
Please enter the identity driver name: CorpMain
Please enter the new password for the driver: *******
TppConfiguration: Venafi Account user Admin requested to change the service
  account password for identity connector 'CorpMain'
TppConfiguration: Venafi Account user Admin successfully changed service
   account password for identity connector 'CorpMain'
```

To use a script to update the service account password

1. (Optional) For TppConfiguration help such as syntax or return codes, type*[Venafi installation folder]\Platform TppConfiguration -help*.
2. In your script, call the TppConfiguration.exe utility and use the following switches:

Switch	Description
-driverpwd:	The new service account password.
-name:	The common name of the identity driver.
-username:	The Trust Protection Platform local, master administrator account name.
-password:	The Trust Protection Platform local, master administrator password.

For example:

```
TppConfiguration.exe -driverpwd:newpassword
-name:CorpMain -username:admin -password:LetMeIn1$
```

Response:

```
TppConfiguration: Venafi Account user Admin requested to change the
  service account password for identity connector 'CorpMain'
TppConfiguration: Venafi Account user Admin successfully changed
  service account password for identity connector 'CorpMain'
```

For more details about the TppConfiguration command-line utility, see "Using the TppConfiguration command line tool" on page 511

About API integrations

To run properly, your client applications must integrate with Venafi. Integration requires a master administrator to register the client and assign API access to allow OAuth token usage. The API Integration wizard helps you manage API access.

The wizard requires:

- The identity of the REST API caller(s).
- One or more scopes and restrictions that represent the set of API calls that the client will make.

DID YOU KNOW? Proper integration is necessary. Otherwise, API calls that are out of scope can fail at run time.

Token terminology

Scope

A range of one more scopes that represent the set of API calls that a client will make. If the endpoint updates a resource, be sure to include the required *restriction*. The most commonly used scopes are listed below. However, the wizard can import any required scope:

- **Admin**: API calls that help you manage the application. For example GET Log/LogSchema.
- **Agent**: API calls that access to Agent resources. For example, GET Client/Details.
- **Certificate**: API calls that manage certificates. For example, POST Certificates/Request.
- **Code Sign:** Admin API calls to CodeSign Protect endpoints. For example, POST Codesign/CreateApplication.
- **Codesignclient**: CodeSign Protect signing endpoints. For example, POST API/Sign.
- **Configuration**: Basic management tasks that require policy, metadata, engine, or workflow. For example, POST Config/Find.
- **Restricted**: Low level work such as SecretStore/LookupByVaultType.
- **Security**: Credentials and permissions. For example, POST Credentials/Delete.
- **SSH**: SSH key or certificate task. For example, POST SSH/KeysetDetails.

Restriction
: The part of a scope that allows endpoints to update or change Venafi resources. If the endpoint supplies read-only data, it may not have a restriction.

Token
: The OAuth grant that allows the client application to make API calls. Requires an API Auth call that includes a *scope* parameter that matches API Application Integration wizard settings.

Who does what?

More than one person may be responsible for managing client integrations and access:

- The developer supplies a list of anticipated API calls and matching scopes and restrictions. The best way to find this information is in the Scope map for tokens in the *Developer's Guide*.
- As administrator, you use the API Application Integration wizard to register and manage scopes.
- The developer will use those same settings in a REST Authorize call that requests a token from the VEDAuth server.
- After VEDAuth responds with a token, the developer or client adds the token in the header of every API call . The token is valid until it expires or the grant is revoked.

- If scope requirements change, you recreate or update the registration. Otherwise, API calls may fail at runtime. After the change, the client can revoke and get a new token.
- After the client completes its work, it can make a REST API call to revoke the token.

Integrating other systems with Venafi products

Every API integration needs to register with Venafi. Registering your Integration allows the client to get an OAuth access token and refresh token with permissions to the REST API endpoints your integration needs. API calls automate your work. By default, all Venafi products, utilities, and other open-source projects are pre-registered. You only need to register integrations from the Venafi Marketplace or your own custom-built integrations.

How does it work?

The API Integration wizard registers details about API calls that the client will make. After registration, the client requests a REST authorization using that same information. The VEDAuth service responds with an access token to allow the client to make API calls. The token is valid until it expires or is revoked.

If configured for your integration, you also get a refresh token. When a token expires, the refresh token allows you to get an access token from the same grant. Refresh tokens allow you to get new tokens without re-authenticating to the VEDAuth service. A refresh token is valid only once and it remains valid until your grant expires.

First things first

- Familiarize yourself with OAuth terms and the flow process. For more information, see "About API integrations" on page 750.
- From the developer, get a list of scopes and restrictions based on the integration's needs. Need help? Use this basic chart.

Scope and Developer Example	Privileges and Restrictions					
	Approve	Delete	Discover	Manage	Revoke	[Other]
admin *scope: admin:recyclebin,delete*					✓	recyclebin
agent *scope: agent:delete*		✓				
certificate *scope: certificate:approve,delete,discover,manage,revoke*	✓	✓	✓	✓	✓	
codesign *scope: codesign:approve,delete,manage*	✓	✓		✓		
codesignclient *scope: codesignclient*						This is a read-only privilege.
configuration *scope: configuration:delete,manage*		✓		✓		
restricted *scope:restricted:delete,manage*		✓		✓		
security *scope: security:delete,manage*		✓		✓		

Scope and Developer Example	Privileges and Restrictions					
	Approve	Delete	Discover	Manage	Revoke	[Other]
ssh *scope: ssh:approve,delete,discover,manage*	✓	✓	✓	✓		
statistics (requires Vendor integration) *scope:statistics*						This is a read-only privilege.
(**Read access**) Specify a scope. *scope:certificate* (**Many scopes**) Use a semi-colon (;) between each scope. *scope:ssh*; *certificate:discover,manage*; *configuration:manage*						

To register (create) a new integration

1. If you've not done so, set the expiration and refresh time for tokens. See Setting up token authentication in the *Developer's Guide*.
2. From the Platform menu bar, click **API** > **Integrations**.
3. Do one of the following:

   #### All of the scopes We need appear in the table (above)

   a. Select **New**.

   b. In **Overview**, complete the form. If you want the client **Name** and **Client ID** to match, leave **Client ID** blank. Click **Next**.

   c. In **Base access**,select the **Scope** and its corresponding **Privileges and restrictions** (if any).

Read is an implied restriction that is automatically given with any scope. So endpoints that are read-only will automatically have access via a token, even if there are no restrictions given. The settings should match the developer's list of API calls that the client will use. If a scope or restriction is missing, restart the wizard and use the Import option to specify the needed scopes.

For example: my integration discovers certificates and logs progress. It needs `certificate` scope with `manage` and `discover` restrictions. I also select `log` scope with `manage` and `delete` restrictions.

d. (Optional) To override token refresh settings, click **Use global default settings**, customize the days, hours, or minutes, and then click **Next**.

e. In **User or team access**,search for people or service accounts who will be running your integration. Then click **Add**.

f. Click **Done**.

Special scopes/Restrictions including Venafi Market Place integrations

a. Click **Import**.

b. Paste the JSON from your integration. The `id` is your client_id for Authorize REST calls. You can also use any of the scopes that appear in the table (above). For example:

Example JSON

```
{
   "id":"My Integration",
   "name":"Its name",
   "vendor":"My company",
   "description":"Purpose",
   "scope": "admin:approve;codesign:admin,manage,delete"
}
```

c. (Optional) To download the integration on your computer, click **Create**.

d. To save, click **Quick Create**.

e. Use the wizard to set any other fields such as user or team access.

f. Click **Done**.

What's next?

- From the Overview tab, copy and give the JSON to the developer. The developer customizes the JSON to request a token via an Authorize method, such as POST Authorize/OAuth in the Developer's Guide.
- Later, if you need to make changes, see"Updating integration registrations" on page 758

API Integrations inventory

The API integrations inventory debuts Venafi Platform's next generation inventory and filtering list.

There are two views of the inventory:

- **Table view.** In the table view, the list of items includes columns that display additional information about each item. This view is most similar to the traditional inventory list you may be familiar with from Venafi Platform's previous inventories.
- **Detail view.** The details view shows an overlay of a specific item from the inventory, providing a detailed view of the selected item. In this view, you can update, export, or delete an integration. You can also use the pagination icons to move to other inventory items.

To create an new integration or to import an integration from another engine, click **Add**.

Searching and filtering the table

Use the search box to search for terms across multiple fields. You can search on any column displayed on the page. The search box is not for creating advanced queries. Use the Filters button to create advanced queries with operators.

If you have a filter applied, you will see a bubble with the number of filter criteria on the **Filters** button. If you use the Search box while a filter is applied, the Search box will only search items that match the applied Filter criteria.

Click **All Integrations** to see a list of saved filters. For information on saving and managing filters, see "Creating, saving, and modifying inventory filters" on page 761.

Customizing the table view

The table has several features to make managing the inventory easier, including:

- Sorting by column. Hover over a column header to see the sort button. Click it once to sort by that column. Click it again to reverse the sort order. Click it a third time to remove the sort.
- Table pagination. Some inventories can contain many items. Venafi Platform uses table pagination to increase performance and reduce load time. You can use the **Rows per page** setting to control how many items you want to view at once. (A larger number of rows will load more slowly than a smaller number of rows.) There are right and left arrows to let you browse from page to page.
- **Columns** button lets you choose which columns you want to display in the inventory . These settings are persistent from session to session, but only affect your account.
- **Density** button lets you control the spacing between rows.
- **Export** button lets you save a CSV file of the entire integrations page. All rows are exported, but only the displayed columns are exported.
- Column settings. Hover over a column name and click the More menu (three stacked dots) to see the column action panel, which are additional tasks you can do with the column, including sorting, filtering, and pinning.

Inventory Accessibility features

To navigate the inventory using the keyboard:

- Tab to the table by pressing the TAB key to move forward (or SHIFT + TAB to move backwards) until the first column heading has focus.
- When a checkbox has focus, press the SPACE key to select or deselect the row.

When inside the table:

Key	Description
Arrow keys (up, down, right, left)	Navigate between cells.
HOME	Navigate to the first cell in the current row.
END	Navigate to the last cell in the current row.
CTRL + HOME	Navigate to the first cell of the first row.
CTRL + END	Navigate to the last cell of the current row.
SPACE (or PAGE DOWN)	Navigate to the next scrollable page.

Key	Description
PAGE UP	Navigate to the previous scrollable page.
CTRL + A	Select all rows (for multi-row actions).
TAB	Leave table to navigate to next control outside the table
SHIFT + TAB	Leave table to navigate to previous control outside the table.

When a column heading has focus:

Key	Description
ENTER	Cycle through the sort options for that column.
CTRL + SHIFT + ENTER	Open the column's action panel.

Details view. Top open the Details view, navigate to an item in the **Name** column, then press ENTER. Once in the details view:

Key	Description
TAB	Move between controls.
ENTER or SPACE	Activate the control.
Arrow left and Arrow right	When one of the tabs (like Overview) has focus, use the arrow keys to move between tabs, then press TAB to move to controls on the tab.
ESC	Close the modal window and return to the previous screen.

Updating integration registrations

The **API Integrations** page manages registered integrations. The **People with active grants** column is the total number of users who have a valid token. The token grants the user the right to run the integration. The **Active grants** column is the total number of issued tokens that your integration received. When tokens are revoked or the grant expires, the number of grants decreases.

To update existing integration registrations

1. From the Platform menu bar, click **API** > **Integrations**.
2. To limit the search to a subset of integrations, click **All Integrations** and make a selection. This is where you can see any saved filters.

3. Locate the integration you want to update using searches or filtering, if desired.
4. Click the name of the integration you want to modify.
5. On any of these tabs, make your changes, and then click **Save**:
    - **Overview**: You can only change details for your own integrations. Venafi and technology partner integration overview information is read-only.
    - **Base access**: You can only change scopes for your own integrations. Venafi and technology partner integration scopes are read-only.

      > **TIP** When you add scopes or restrictions, the token with the original grant is still valid until it expires or it is revoked. Your developer should revoke the original grant and request a new grant with the new scopes or restrictions.

    - **User and team access**: Locate the identity that represents a person, team, or machine. To remove access for a user or team, click the trash icon in their row. To add a user or team, use the User or team search box to find the account(s) then click the box to select the account. Click Add, then click Save. If your identity list is covering the Add button, click outside the drop-down list to return to the main view. For more information see "Revoking user and integration grants" on the next page.

> **WARNING!** Be careful about updating existing integrations. If you remove scopes or privileges and restrictions from a working integration, the application that relies on that integration may break. It's usually better to create a new integration with the scope, privileges, and restrictions needed, and use that going forward.

JSON updates from integration owners

Sometimes integration owners will need to update their integrations, and will provide you with JSON-formatted code to use for the update.

> **IMPORTANT** If you update the scopes and restrictions for an existing integration, the systems that rely on the integration may stop functioning because their grants may no longer match the changes provided. If you update the JSON for an API integration, your developer should revoke the original grant and request a new grant with the new scopes and restrictions.

To update an API integration using JSON

1. From the Platform menu bar, click **API** > **Integrations**, then locate the API integration you want to update.

2. Check the box next to the integration you want to update, then click **Update**.
3. Paste the JSON into the text box.
4. Check the box stating you understand the risks of updating an integration and want to continue.
5. Click **Update**.

Revoking user and integration grants

If a person leaves the company, you might want to remove their identity entry from the integration. There are two ways to revoke the integration's access to Venafi APIs. Either use the Identity tree or the API Integration page. If you use the API Integration page, the token is still valid until the grant expires. After grant expiration, access is denied and they will not be able to refresh the token to get a new grant.

To immediately revoke user grants for registered integrations with Venafi, see "Revoking a user's access grant" on page 700.

To revoke refresh capability for a specific API integration

IMPORTANT Removing identities doesn't affect existing grants or tokens for the API integration but only limits the identities you've removed from getting *new* grants to the API integration.

1. From the Platform menu bar, click **API** > **Integrations**.
2. In the left navigation, click an integration, and then click **Users or team access**.
3. Under **User/Team**, click the trash icon.
4. Click **Save**.

   All preexisting grants and tokens remain active until the token expires. After expiration, the user or group will not be allowed to refresh the token to gain access to the integration.

Deleting API integrations

When an integration is no longer in use, you can remove it from the API Integrations list. You should only delete your organization's own integrations from the list. Venafi integrations, which automatically appear in the list, CAN be deleted. However, they will automatically be re-added next time you perform a patch or upgrade. When you remove the integration, you un-resgister it from the VEDAuth server and any corresponding tokens and grants are no longer valid.

To delete an API Integration

1. From the Platform menu bar, click **API** > **Integrations**.
2. Select one or more integration names for the integrations you want to delete.
3. Click **Delete**.
4. To confirm, follow the instructions.

Exporting an API integration

If you want to share an API integration with another server in your cluster, you can easily export a JSON file of the integration configuration that you can later import to another system.

You can also use this feature to share an integration with the wider Venafi Warrior community.

To export an API Integration

1. From the Platform menu bar, click **API** > **Integrations**.
2. Click the **action icon** in the row of the integration you want to export (or open the details pane and click **Export**.)
3. Click **Export**.
4. Click **Copy JSON**.
5. Paste the JSON into the desired application.
6. Click the **X** to close the modal window.

Creating, saving, and modifying inventory filters

> **NOTE** This topic refers to the new inventory introduced on the API Integrations inventory in 22.2. Other inventories will eventually be migrated to this new style.

You don't always have to start browsing for items from scratch. You can create a filter that helps you find the items that you are interested in, and you can save that filter.

If you have a saved filter, you can make it your default filter, which will load each time you open the page.

For example, if you are looking at a list of certificates, your default filter might be "All Certificates."

To create a filter

1. Use the **Filters** button to narrow the list using criteria you will define below.
2. For each filter criteria, select the **column**, the **operator**, and the filter **value**.
3. [Optional] To add additional filter criteria, use the **Add Filter** button, and choose the operator (either **AND** or **OR**).
4. [Optional] To remove a criteria row, click the X icon on the left.
5. The filter applies as you update the criteria, helping you know if your criteria are producing the result you expect.

The Filters button shows a bubble showing the number of criteria currently being used to filter the inventory.

To save a filter

1. Create the filter as described in the previous section.
2. Click **Save Filter**.
3. Enter a name for the filter.
4. If you want this to be the default filter that is used when the inventory loads, check the box.
5. Click **Save**.

To change your default filter

1. On the filter bar, click the saved filter drop-down. (This is the button to the right of the search filter box. It's name is whatever saved filter is being used.)

   For example, if you are filtering certificates, the default saved filter is probably "All Certificates", so click that drop-down.
2. Click **Manage Filters**.

   In the **Manage Filters** window, the filters at the top of the list are default and can't be changed. The filters you have saved are listed in the **My Filters** group.
3. On the list of filters, click the flag icon next to the new default.
4. Click **Save**.

The next time you load the list, your default filter will be applied automatically.

To delete a saved filter

1. On the filter bar, click the saved filter drop-down.

   For example, if you are filtering SSH keys, the default saved filter is probably "All Keys", so click that drop-down.

2. Click **Manage Filters**.

   In the **Manage Filters** window, the filters at the top of the list are default and can't be deleted. You can only delete the filters in the **My Filters group**.

3. Click the trash icon next to the filter or filters you want to delete.

   > **NOTE** The filter will show **Pending Deletion**. If you were to click **Cancel** the filter would not be deleted.

4. Click **Save**.

API default settings for remote access configuration

Applications that need to connect to Venafi Platform are configured on the "API Integrations inventory" on page 756 The API Default Settings page allows you to configure the default remote access settings that apply to all API integrations, unless they are overridden for a specific application.

To configure these settings, go to the Platform product menu bar, and click **API** > **Default Settings**.

Alternate methods of completing these tasks

If you have access to the Venafi server you can also complete these tasks in Venafi Configuration Console. For information, see "Access Management" on page 389

If you have access to a Venafi MMC snap-in, you can also complete these tasks there. The instructions are the same as for the Venafi Configuration Console, above.

If you have access to the Web SDK, you can modify these settings via the API `Authorize` and `OAUTH` endpoints. For example, to configure certificate authentication via API, see POST Authorize/Certificate.

Authentication Methods

API applications need to authenticate to the Venafi Platform database. The Authentication section allows you to specify which authentication method(s) you want to support for remote access by APIs.

Authentication	Trust Protection Platform Authentication Server setting
Username & Password	The client passes a user name and password to the VEDAuth server. Recommended for POST Authorize/OAuth.
Integrated MS Windows Authentication	Default. The client passes Windows credentials to the VEDAuth server.
Browser-based authentication	Default. Required for POST Authorize/Device. Recommended for multi-factor SAML authentication: ■ **Enabled**: Default. Allow multi-factor authentication for devices. A successful response, includes a web link to complete the authentication. ■ **Disabled**: Block browser-based authentication.
JSON web token	A token in JSON format that is used to communicate between a trusted identity provider and Venafi Platform.
Certificate	The caller passes a client certificate to the VEDAuth server. When selected, the **Use AD Security Identifier (SID) value if available** option appears.
AD Security Identifier (SID)	If you select Certificate, the **Use AD Security Identifier (SID) value if available** option appears. In this scenario, AuthServer follows a specific process. First, it looks for the SID Extension value in the certificate. If the SID Extension is found, AuthServer tries to find the matching AD user. However, if the SID Extension is not in the certificate or doesn't match an AD account, AuthServer will then use the "Location" setting as a backup.

If you select the Certificate authentication method, you might need to configure the following settings:

Field	Parameter
X.509 Identity Field	The field for Trust Protection Platform Authentication Server to use as the user identity: ■ **SubjectAltName: UPN**: The identity that also has access to the Web SDK. ■ **SubjectAltEmail**: The email address (es). ■ **CN**: The certificate name (CN). For local identities, always specify *CN*.
Trusted Certificate Authorities	The CA(s) that are approved to issue client certificates for authentication. Select a Trusted Certificate Authority certificate from the Roots tree.
AD Security Identifier (SID)	The certificate is mapped to the Active Directory User's SID (objectSid).

Token settings

There are two validity periods for API authentication access to Venafi Platform API endpoints: access grants and tokens.

- **Access grants.** This is the duration of time that the application will be able to access Venafi Platform. After the application access expires, an administrator will need to create a new application.

  Access grants have a minimum validity period of fifteen minutes.

- **Tokens.** This is the duration of time between authentication prompts. Tokens automatically expire when the access grant expires. This setting allows you to have increased security by requiring periodic authentication to the system. When a token expires, if the access grant is still valid, a user can obtain a new token.

  Tokens have a minimum validity period of one minute.

To use different expiration times for tokens and access grants, enable the **Token refresh** option, then set a value for both token expiration and access expiration. When you disable the Token refresh option, then the same value is used for both token expiration and access expiration. In this case, the minimum validity period is one minute.

The token validity cannot be shorter than the access grant.

Session Caching

The session caching settings control how API session credentials are cached in Venafi Platform.

There are three settings:

- **Expiration mode**. Using **normal mode**, credentials are cached for up to five minutes. This saves the significant time it takes to check the status of the credential on every single API call. If stringent security is more important than performance, you can enable **strict mode** which forces Venafi Platform to validate the credential on every API call.

  > **IMPORTANT** In internal testing, Venafi noted that the time to execute and return an API response can be over 40% higher when using strict mode.

- **Session pool size.** The number of concurrent sessions for API calls. If the number of simultaneous API calls exceeds the pool size, the oldest unused session is removed from the pool.
- **Session expiration.** The number of minutes each token remains in memory.

12

Configuring the Venafi Trust Protection Platform server object

The Venafi Trust Protection Platform™ server object represents a physical server where one or more Trust Protection Platform program modules are installed. The Trust Protection Platform Server object configuration allows you to manage general server functions such as the time the server runs its daily tasks and how often it checks for work.

This chapter contains the following topics:

Configuring the Trust Protection Platform server 768

Trust Protection Platform server configuration 768

About using an HTTP proxy 784

Configuring the Trust Protection Platform server

The Trust Protection Platform server object configuration allows you to manage general server functions such as the time the server runs its daily tasks and how often it checks for work.

To configure the Trust Protection Platform server object

1. From the Platform menu bar, click Policy Tree.
2. Select the **Platforms** tree from the Tree drop-down menu.
3. In the Platforms tree, select the Trust Protection Platform server that you want to configure.
4. Configure the Trust Protection Platform server settings.

   For reference, see "Trust Protection Platform server configuration" below.
5. When you're finished, click **Save**.

Trust Protection Platform server configuration

The following settings are available for Trust Protection Platform servers. These settings vary based on global or individual server configuration:

- Global server settings are available on the Platforms Engine tab.
- Individual server settings are available on the Platforms *[serverName]* page.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
ACME Server tab	Settings		Root Platforms object	The settings in this tab are available from the root **Platforms** object.
		Settings		The check boxes allow the ACME server to be enabled and folders to be automatically created if they don't exist. See *ACME integration with Trust Protection Platform*.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
Authentication	Settings		Root Platforms object	The settings in this tab are available from the root **Platforms** object.
		Authentication		**Certificate Authentication**: The check box to allow certificate authentication. Additional configuration is required. For more information, see "Setting up certificate authentication for web console" on page 793. **Also Require User Password**: The check box to allow a user password for authentication.
Certificate Manager	Settings		Root Platforms object	The settings in this tab are available from the root **Platforms** object.
		Trust Store Management		**Disabled**: The setting for Trust Store Management. The default is *No* (continue Trust Store Management of the certificate).
Certificate Revocation	Settings	Settings	Root Platforms object	**Check-in interval (times daily):** The number of times each day that you want Trust Protection Platform to check the CRL endpoints to update the CRLs and check revocation of certificates in the inventory.
Network Device Enrollment	Settings		Root Platforms object OR child object	The settings in this tab are available from the root **Platforms** object or child object.
		General		The Network Device Enrollment tab is available only in Policy Tree.The Network Device Enrollment tab enables Simple Certificate Enrollment Protocol (SCEP) certificate enrollment on the Trust Protection Platform server.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				When Network Device Enrollment is configured, Venafi TLS Protect can receive a CSR from a SCEP-enabled device, renew the certificate with the appropriate CA, then allow the device to download the renewed certificate from the Trust Protection Platform server. As a non-CA-based certificate enrollment solution for SCEP systems, Trust Protection PlatformTLS Protect can manage certificate enrollment with multiple CAs using multiple CA templates. Additionally, Trust Protection PlatformTLS Protect provides a robust system of hierarchical, policy-based rules that allow administrators to manage where Certificate are created in the Policy tree. For details on network device enrollment, see About network device enrollment in the *Venafi Trust Protection Platform Certificate Management Guide*. For specific information on the fields available in this section, see Network Device Enrollment Settings–Platform Object.
Platforms			Root Platforms object	
	Settings	Global Options (Impacts all users)		**Automatically apply filter parameters on certificate inventory:** By default, the certificate inventory does not automatically load until you click the Apply Filters button. This applies both on loading the certificate inventory page, as well as when you add individual filters to the page. This is especially helpful for large certificate inventories that take longer to load. If you prefer the previous behavior, which is to load the inventory on page load, you can enable this option. You must reset IIS after changing this option.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				Support large object trees: Control the view of the Policy tree for all users. When enabled, hide all objects and show only search results via Query mode. When disabled, show all Policy tree objects. If you want this search feature for certain users, set the values on the User Preferences Appearance tab. **Enable team creation by everyone:** When checked, any user can create a team. **Enable Management Type verification:** When checked, certificates set with "Provisioning" management type are checked to see if there is an installation/application association. When this feature is enabled, you can filter the certificate inventory on a risk called "No Provisioning Targets" to see certificates set for provisioning but that don't have an application. If you try to save a certificate set for provisioning, but without an application, Venafi Platform will warn you, and suggest you change the type to "Monitoring". For more information, see Certificate status and risks explained.
		Allowed Outbound SSL/TLS Versions		One or more protocols to control outbound communications with other servers. ■ **SSL 3.0**: Allow or block Secure Socket Layer (SSL) 3.0 communications. Recommendation: Unchecked (block). ■ **TLS 1.0**: Allow or block (TLS) 1.0 communications. Recommendation: Unchecked (block). ■ **TLS 1.1**: Allow or block (TLS) 1.1 communications. Recommendation: Unchecked (block).

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				■ **TLS 1.2**: Allow or block (TLS) 1.2 communications. Recommendation: Checked (allow). ■ **TLS 1.3**: Allow or block (TLS) 1.3 communications. Recommendation: Checked (allow). Whenever you modify these settings, you must reset IIS. **CAUTION** By default, only TLS 1.2 is selected, which is the recommended best practice from a security perspective. However, if you have applications that cannot connect using TLS 1.2, you will need to assess your best options. Using the Venafi-recommended options may reduce compatibility, especially with older applications. For additional information, we recommend the following documentation from Microsoft: TLS, DTLS, and SSL protocol version settings.[1] **IMPORTANT** Syslog channel drivers can't recognize changes you make to either the **Allowed Outbound SSL/TLS Versions** settings or **Certificate Versions** settings. Therefore, following any changes to those settings, please restart the Venafi Log Server Windows service. For details, see "Manually stopping and starting the log server service" on page 432 in the *Log Server Administration Guide*.

[1] Available at: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#tls-dtls-and-ssl-protocol-version-settings

Tab	Sub-tab	Feature or section	Appears on	Option and Description
	Engine	Global Options		**Run daily tasks at** The time that the Trust Protection Platform server runs daily tasks. Daily tasks include the Certificate, SSH Key, and Symmetric Key monitoring scans and Validation scans. **NOTE** If Trust Protection Platform does not have enough resources to process the daily tasks, an event generates. The event indicates that the engine failed to complete daily tasks in a 24-hour period. The event generates in extenuating circumstances when there are too many Work To Do items in the queue. To monitor these kinds of events, you can create a Notification Rule. **NOTE** Normally, Trust Protection Platform runs daily validation scans. However, if a user clicks the  Validate Now option in a Certificate or Application object, the validation scan queues the Validation module for an immediate scan. For more information, see Running Validation Scans in the *Venafi Trust Protection Platform Certificate Management Guide*.
		Certificate Verification Settings		**Verification Mode**: The level of certification verification to use to establish the HTTPS connection with a server that has a certificate: ■ **None (Not Recommended) - No verification**: (Default) Allow the connection to the server. If the certificate would have failed the Basic or Strict certificate verification, log a Certificate Verification Warning event message.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				■ **Basic - Checks expiration, revocation, common name mismatch & root chain**: Check for an expired certificate, CN mismatch, invalid chain, inability to chain back to a trusted root, and whether one or more of the certificates in the chain has an invalid CA certificate. If any of these checks are invalid, refuse the connection and log a Certificate Verification Failed event message. If the certificate would have failed the Strict certificate verification, log a Certificate Verification Warning event message. ■ **Strict (Recommended)- Basic checks & Server Authentication EKU**: Do the same checking as with the Basic certificate verification. Reject a certificate if it failed the Basic certificate verification. Also, if the Server Authentication (EKU) is present on the certificate, verify the value. Reject an otherwise valid server certificate that lacks the Server Authentication Purpose information in the EKU. For rejected certificates, refuse the connection with the server and log a Certificate Verification Failed event message. **Check CRL**: The setting to determine whether the server certificate appears on a Certificate Revocation List (CRL). CRL checking occurs prior to making the HTTPS connection. Use this setting in conjunction with *Verification Mode*: ■ **Never**: Bypass CRL checking. Establish the HTTPS connection based on certificate values. ■ **When Possible**: (Default) If the certificate is valid, determine whether it is currently on the CRL. If the certificate is revoked, refuse the connection and log a Certificate Verification Error event

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				message. However, if the CRL cannot be retrieved, allow the connection. ■ **Always**: If the certificate is valid, always determine whether it is currently on the CRL. If the certificate is revoked or cannot be verified on the CRL, refuse the connection. Log a Certificate Verification Failed event message. For more information, see "Setting up Certificate Verification for securing outbound HTTPS connections" on page 839. **IMPORTANT** Syslog channel drivers can't recognize changes you make to either the **Allowed Outbound SSL/TLS Versions** settings or **Certificate Versions** settings. Therefore, following any changes to those settings, please restart the Venafi Log Server Windows service. For details, see "Manually stopping and starting the log server service" on page 432 in the *Log Server Administration Guide*.
		Trust Protection Platform URL HostNames		■ **Aperture**: The setting for the $ApertureFQDN$ macro. Type the fully Qualified Domain Name for an Aperture host, for example `aperture.venafi.com`. If the attribute value is not set, the macro returns the $HostName$ value instead.

Tab	Sub-tab	Feature or section	Appears on	Option and Description

> **NOTE** Do NOT include the protocol (`https://`), or the `/Aperture` directory. Just enter the FQDN itself. So, if your Aperture URL is `https://platform.venafi.com/Aperture`, you would enter:
>
> platform.venafi.com

This setting is critical for configuring SAML SSO (single sign-on), because since most organizations use some type of load balancing software, the system can't determine its own FQDN, yet the FQDN used by the cluster must match the FQDN found in the `common name` or `DNS Subject Alternative Name` of your CA-issued Venafi Operational Certificate (VOC) so users don't encounter a certificate error when logging in via SAML.

- **Client Subsystem for Agents**: The setting for the $VEDClientFQDN$ macro. Type the fully Qualified Domain Name for the Client Subsystem for agents, for example client.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead.

- **Network Device Enrollment**: The setting for the $SCEPFQDN$ macro. Type the fully Qualified Domain Name for the SCEP host, for example scep.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead.

- **REST API**:The setting for the $WebSDKFQDN$ macro. Type the fully Qualified Domain Name for

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				the Web SDK host, for example websdk.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead ■ **Policy Tree**The setting for the $WebAdminFQDN$ macro. Type the fully Qualified Domain Name for the Web Admin host, for example webadmin.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead.
	Proxy	Proxy Settings		**Use Configured Proxy**: Configures Trust Protection Platform to use the Windows default proxy server as it is configured on the Trust Protection Platform server. If you select this option, you do not have to configure the **Proxy Host**, **Port**, or **Credential** fields. **Host**: The Hostname or IP address of the proxy server Trust Protection Platform uses to connect to the Internet. Trust Protection Platform supports both IPv4 or IPv6 connections. Port: Port the proxy server uses for client connections. **Credential**: Username Credential required to connect to the proxy server. **NOTE** If your proxy server uses domain authentication, make sure the Username Credential object is defined using Domain Name or User Principal Name syntax.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				Bypass For Local: Configures Trust Protection Platform to bypass the proxy server for connections to local CAs. Trust Protection Platform uses the following criteria to identify local and external addresses: ■ Hostname is considered as a local address. Everything else is an external address. ■ URL with a hostname is considered as a local address. For example, http://intranet is a local address. ■ URL with a domain name is considered as a Fully Qualified Domain Name and is passed through the proxy server, even if it is a local address. For example, http://intranet.mynetwork.local still passes through the proxy server, even if **Bypass for Local** is selected. ■ URL with an IP address is considered as an external resource, even if it is in the local subnet, and is passed through the proxy server, even if **Bypass for Local** is selected. For example. http://192.168.0.100 (which is the same as http://intranet) is considered as an external resource and is passed through the proxy server.
Venafi Trust Protection Platform			Child objects	
	Settings	Settings		**Run daily tasks at** The time that the Trust Protection Platform server runs daily tasks. Daily tasks include the Certificate, SSH Key, and Symmetric Key monitoring scans and Validation scans.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				NOTE If Trust Protection Platform does not have enough resources to process the daily tasks, an event generates. The event indicates that the engine failed to complete daily tasks in a 24-hour period. The event generates in extenuating circumstances when there are too many Work To Do items in the queue. To monitor these kinds of events, you can create a Notification Rule.
				NOTE Normally, Trust Protection Platform runs daily validation scans. However, if a user clicks the  Validate Now option in a Certificate or Application object, the validation scan queues the Validation module for an immediate scan. For more information, see Running Validation Scans in the *Venafi Trust Protection Platform Certificate Management Guide*.
		Certificate Verification		**Verification Mode**: The level of certification verification to use to establish the HTTPS connection with a server that has a certificate: ■ **None (Not Recommended) - No verification**: (Default) Allow the connection to the server. If the certificate would have failed the Basic or Strict certificate verification, log a Certificate Verification Warning event message.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				■ **Basic - Checks expiration, revocation, common name mismatch & root chain**: Check for an expired certificate, CN mismatch, invalid chain, inability to chain back to a trusted root, and whether one or more of the certificates in the chain has an invalid CA certificate. If any of these checks are invalid, refuse the connection and log a Certificate Verification Failed event message. If the certificate would have failed the Strict certificate verification, log a Certificate Verification Warning event message. ■ **Strict (Recommended)- Basic checks & Server Authentication EKU**: Do the same checking as with the Basic certificate verification. Reject a certificate if it failed the Basic certificate verification. Also, if the Server Authentication (EKU) is present on the certificate, verify the value. Reject an otherwise valid server certificate that lacks the Server Authentication Purpose information in the EKU. For rejected certificates, refuse the connection with the server and log a Certificate Verification Failed event message. **Check CRL**: The setting to determine whether the server certificate appears on a Certificate Revocation List (CRL). CRL checking occurs prior to making the HTTPS connection. Use this setting in conjunction with *Verification Mode*: ■ **Never**: Bypass CRL checking. Establish the HTTPS connection based on certificate values. ■ **When Possible**: (Default) If the certificate is valid, determine whether it is currently on the CRL. If the certificate is revoked, refuse the connection and log a Certificate Verification Error event

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				message. However, if the CRL cannot be retrieved, allow the connection. ■ **Always**: If the certificate is valid, always determine whether it is currently on the CRL. If the certificate is revoked or cannot be verified on the CRL, refuse the connection. Log a Certificate Verification Failed event message. For more information, see "Setting up Certificate Verification for securing outbound HTTPS connections" on page 839.
		Operations		**Certificate**: The DN for the Venafi Operational Certificate. The default value is \VED\Policy\Venafi Operational Certificates\[Engine Name].
		Logging		**Log Debug**: The check box to allow the Log server to store debug information. For more information about Log servers, see"Managing the log server" on page 429.
		Discovery Zones		**Discovery Zones**: The range of Class C or smaller IPv4 addresses to which the current server has physical access. This option allows you to manage the servers to process discoveries. For example, if you have one Discovery Server inside the firewall to run discoveries on private IP addresses and another Discovery Server outside the firewall to run discoveries on public IP addresses, you can define the zones that you want each server to process. For more information on this configuration, see Managing the Discovery Server. If the Discovery module is installed on the current server, it runs discoveries only on the designated zones. If you do not define zones, the Discovery module processes all configured discoveries.

Tab	Sub-tab	Feature or section	Appears on	Option and Description
		Trust Protection Platform URL HostNames		■ **Aperture**: The setting for the $ApertureFQDN$ macro. Type the fully Qualified Domain Name for an Aperture host, for example aperture.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead. ■ **Client Subsystem for Agents**: The setting for the $VEDClientFQDN$ macro. Type the fully Qualified Domain Name for the Client Subsystem for agents, for example client.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead. ■ **Network Device Enrollment**: The setting for the $SCEPFQDN$ macro. Type the fully Qualified Domain Name for the SCEP host, for example scep.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead. ■ **REST API**:The setting for the $WebSDKFQDN$ macro. Type the fully Qualified Domain Name for the Web SDK host, for example websdk.venafi.com. If the attribute value is not set, the macro returns the $HostName$ value instead ■ **Policy Tree**The setting for the $WebAdminFQDN$ macro. Type the fully Qualified Domain Name for the Web Admin host, for example webadmin.venafi.com. If the attribute value is not set, the macro returns the

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				$HostName$ value instead.
		Authentication		**Disabled Identity Connectors:** Use this setting to disable specific identity connectors for a given engine. This allows you to, for example, disable an identity connector on an engine which has no need to resolve identities (like a network discovery only engine).
	Proxy	Proxy Settings		**Use Windows Configured Proxy**: Configures Trust Protection Platform to use the Windows default proxy server as it is configured on the Trust Protection Platform server. If you select this option, you do not have to configure the **Proxy Host**, **Port**, or **Credential** fields. **Host**: The Hostname or IP address of the proxy server Trust Protection Platform uses to connect to the Internet. Trust Protection Platform supports both IPv4 or IPv6 connections. Port: Port the proxy server uses for client connections. **Credential**: Username Credential required to connect to the proxy server. If your proxy server uses domain authentication, make sure the Username Credential object is defined using Domain Name or User Principal Name syntax. **Bypass For Local**: Configures Trust Protection Platform to bypass the proxy server for connections to local CAs. Trust Protection Platform uses the following criteria to identify local and external addresses:

Tab	Sub-tab	Feature or section	Appears on	Option and Description
				■ Hostname is considered as a local address. Everything else is an external address. ■ URL with a hostname is considered as a local address. For example, http://intranet is a local address. ■ URL with a domain name is considered as a Fully Qualified Domain Name and is passed through the proxy server, even if it is a local address. For example, http://intranet.mynetwork.local still passes through the proxy server, even if **Bypass for Local** is selected. ■ URL with an IP address is considered as an external resource, even if it is in the local subnet, and is passed through the proxy server, even if **Bypass for Local** is selected. For example. http://192.168.0.100 (which is the same as http://intranet) is considered as an external resource and is passed through the proxy server.

About using an HTTP proxy

Trust Protection Platform uses HTTP to communicate with several other systems, including certain certificate authorities, certificate revocation list distribution points, and online certificate status protocol responders. Trust Protection Platform supports communication through one or more HTTP proxies if they are required to access HTTP resources.

An HTTP proxy can be configured at the root of the Platforms tree, where it will apply to all Trust Protection Platform engines, or it can be applied to an individual Trust Protection Platform engine.

- Trust Protection Platform respects a system proxy configured in Internet Explorer, which should be set for the user account under which the service is running.
- If an HTTP proxy is configured on an individual Trust Protection Platform engine, that setting will override the setting at the root of the Platforms tree.
- If HTTP proxy settings are locked at the root of the Platforms tree, they cannot be overridden on individual Trust Protection Platform engines.

TIP If your organization has multiple proxy servers with a different addresses and access to different resources, use partitioning and the proxy settings on individual Trust Protection Platform engines to communicate with specific proxies. At the root of the Platforms tree, configure the proxy that will be used by most of the Trust Protection Platform engines but do not lock the proxy settings at the root. Configure one or more Trust Protection Platform engines to use a different proxy. Ensure that the CA Template objects that require access to the different proxies are in the portion of the policy tree that is serviced by these Trust Protection Platform engines.

JWT Mappings operate in tandem with the central proxy configurations set at the root of the Platforms tree. See "About JWT Mappings" on page 402.

Trust Protection Platform's configurable proxy settings

Use Windows Configured Proxy	Configures Trust Protection Platform to use the Windows default proxy server as configured on the Trust Protection Platform engine. If you select this option, you do not have to configure the Proxy Host, Port, or Credential fields. If this value is set at the root of the Platforms tree, each Trust Protection Platform engine will use the proxy settings configured on its local Windows system.
Host	Fully qualified domain name, Hostname, or IP address of the proxy. Venafi TLS Protect supports both IPv4 and IPv6 connections.

Port	IP Port of the proxy
Credential	Username Credential required to connect to the proxy server. If your proxy server uses domain authentication, make sure the Username Credential object is defined using Domain Name or User Principal Name syntax. To select the Username Credential: Click the Browse button. The Credential Selector dialog appears. Select the Username Credential that stores the username and password required to access the proxy server, and then click Select.
Bypass for Local	Configures Trust Protection Platform to bypass the proxy server for connections to local CAs. Trust Protection Platform uses the following criteria to identify local and external addresses: ■ Hostname is considered as a local address. Everything else is an external address. ■ URL with a hostname is considered as a local address. For example, http://intranet is a local address. ■ URL with a domain name is considered as a Fully Qualified Domain Name and is passed through the proxy server, even if it is a local address. For example, http://intranet.mynetwork.local still passes through the proxy server, even if Bypass for Local is selected. ■ URL with an IP address is considered as an

	external resource, even if it is in the local subnet, and will be passed through the proxy server, even if Bypass for Local is selected. For example, http://192.168.0.100 (which is the same as http://intranet) is considered as an external resource and is passed through the proxy server.

For information about configuring an HTTP proxy, see "Configuring an HTTP proxy" below.

Configuring an HTTP proxy

Trust Protection Platform respects a system proxy configured in Internet Explorer, which should be set for the user account under which the service is running. At the root of the Platforms tree, you can configure a single proxy to be used by all Trust Protection Platform engines and HTTP-based services. If your organization has multiple proxies, we recommend that you set the most used proxy address at the top of the Platforms tree and then override that setting with a different address on individual Trust Protection Platform engines.

A proxy can be configured on an individual Trust Protection Platform engine if the proxy setting at the root of the Platforms tree has not been locked. Setting a proxy configuration on an individual Trust Protection Platform engine overrides the value set at the root of the Platforms tree.

JWT Mappings operate in tandem with the central proxy configurations set at the root of the Platforms tree. See "About JWT Mappings" on page 402.

Additional information about using the Microsoft Crypto API revocation checking and proxies

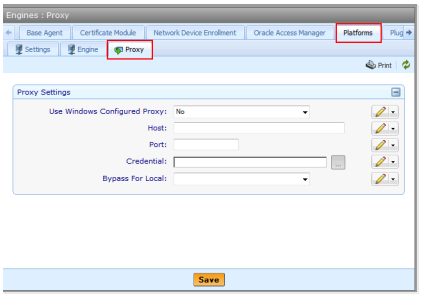
Venafi Platform and the Amazon AWS SDK use the `System.Net.HttpWebRequest` class, which uses the Microsoft Crypto API to perform revocation checking as part of the SSL/TLS handshake.
The MS Crypto API must be configured to use the proxy during revocation checking so that these requests will be performed through the proxy as well.

You may see this issue with any Venafi Platform driver, or in some other areas of Venafi Platform. For more information see the following Microsoft documentation:

- Description of the Cryptography API proxy detection mechanism when downloading a Certificate Revocation list (CRL) from a CRL distribution point.[1]
- Certificate Revocation List (CRL) Chech and WinHttp Proxy settings.[2]

Set a proxy for all Trust Protection Platform engines

1. From the Platform menu bar, click Policy Tree.
2. Select the **Platforms** tree from the Tree drop-down menu.
3. Select the root of the Platforms tree.
4. Select the **Platforms** tab, and then click **Proxy**.
5. Configure the proxy settings.



> **TIP** To prevent a proxy from being set on an individual Trust Protection Platform engine, lock the proxy settings at the root of the Platforms tree.

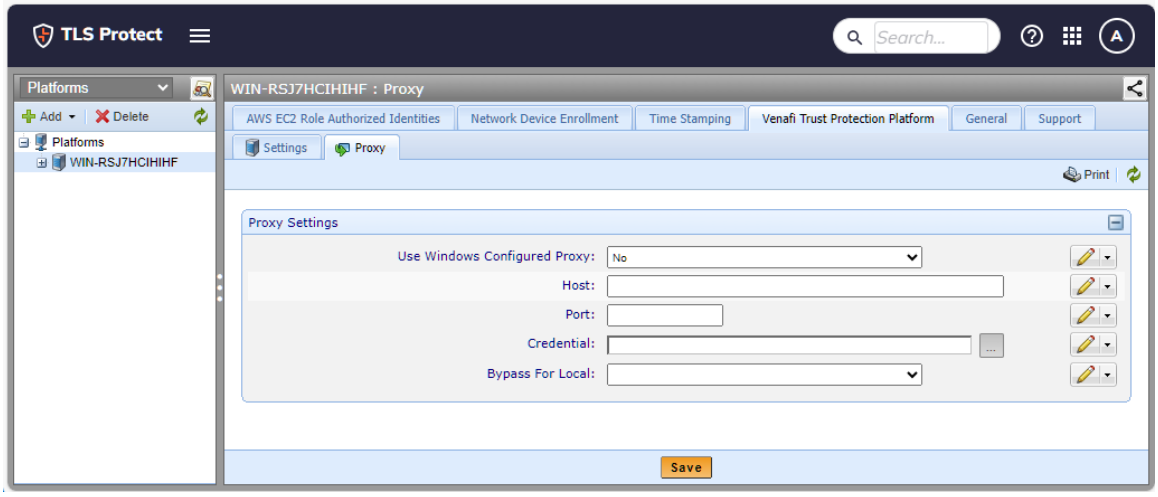
Set a proxy for a single Trust Protection Platform engine

1. From the Platform menu bar, click Policy Tree.
2. Select the **Platforms** tree from the Tree drop-down menu.
3. Select the**Trust Protection Platform** engine that will hold the settings.
4. Select the **Venafi Trust Protection Platform** tab, and then click **Proxy**.

---

[1] https://docs.microsoft.com/en-us/troubleshoot/browsers/description-of-cryptography-api-proxy-from-crl
[2]https://docs.microsoft.com/en-us/archive/blogs/jpsanders/certificate-revocation-list-crl-check-and-winhttp-proxy-settings

5. Configure the proxy settings.



13

Alternate authentication and login options (including single sign-on)

Your users can use a variety of authentication methods to authenticate to Venafi Platform products, including certificate authentication, Windows authentication, and true single sign-on (SSO) authentication.

This section describes how to set up alternate ways to log in to the Trust Protection Platform in place of the native log in.

The web console supports the following authentication methods:

- Default username and password authentication built-in to Trust Protection Platform. You can either use local users (managed within Trust Protection Platform itself), or you can use an identity provider like LDAP or Active Directory to manage your users.
- Certificate-based authentication
- Integrated MS Windows Authentication
- SAML v2 SSO

In addition, the Web SDK supports the following *additional* authentication methods:

- Device authentication
- JSON Web Token (JWT) authentication

This chapter contains the following topics:

Setting up certificate authentication for web console 793

Setting up certificate authentication for API remote access 794

About Integrated MS Windows Authentication 796

Enabling RSA SecurID 802

Oracle Access Manager settings 809

Working with SAML for single sign-on (SSO) 810

Setting up certificate authentication for web console

To configure certificate authentication for the web console, you will also need to configure certificate authentication for API access. Both of these tasks are outlined in the next section.

After you make the necessary configuration settings in Trust Protection Platform, you need to configure Microsoft IIS Manager to accept certificate authentication. For specific steps, see the following procedures.

To enable certificate authentication in Trust Protection Platform for the web console

1. From the Platform menu bar, click **Venafi Servers**.
2. Click on the **Authentication** tab.
3. Check the box for **Certificate Authentication**.
4. Click **Save**.

   This enables certificate authentication for the web console. In the next steps, you will configure the specific settings by enabling and configuring certificate authentication for API users.
5. From the Platform menu bar, click **API** > **Default Settings**.
6. In the **Authentication** section, check the box for **Certificate**.

   Fields specific for certificate authentication are shown.
7. In the **Trusted certificate authorities** field, select which CA(s) you want to use as trusted root CAs for issuing client certificate for authentication.

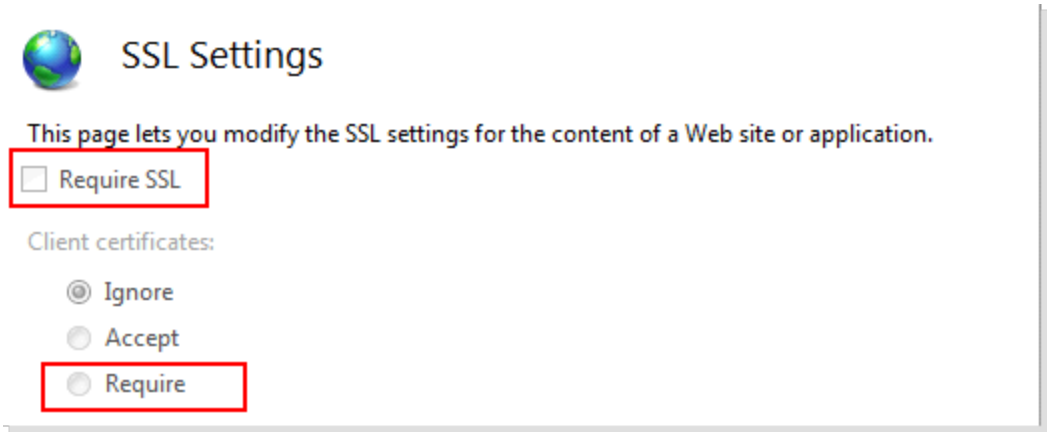
   Use the check boxes to select multiple CAs if needed.
8. Click **Save**.
9. Log out of Venafi Platform.
10. Log back in to Venafi Platform.

    You should see the status message *A valid certificate credential is required to log in.*

Now that certificate authentication has been enabled and configured for web console access, need to configure some settings in IIS.

To Configure IIS Manager to accept certificate authentication for the web console

1. Open **Server Manager** on the Venafi server.
2. Click **Tools**.
3. Click **Internet Information Services (IIS) Manager**.
4. Navigate to **Sites** > **Venafi** > **Aperture**.
5. Click **SSL Settings**.
6. Select **Require SSL**, and then under **Client Certificates**, select **Require**.



7. Click **Apply**.

Setting up certificate authentication for API remote access

Alternate methods of completing these tasks

If you have access to the Venafi server you can also configure certificate authentication for API users in Venafi Configuration Console. For information, see "Access Management" on page 389.

If you have access to the Web SDK, you can modify these settings via the API `Authorize` and `OAUTH` endpoints. For example, to configure certificate authentication via API, see POST Authorize/Certificate

These steps **do not** configure your system to allow end users to use certificate authentication for the web console. That requires additional steps that are described in "Setting up certificate authentication for web console" on the previous page.

There are two parts to setting up certificate authentication: first, you need to enable and configure it in Trust Protection Platform, and second, you need to configure Microsoft IIS Manager to accept it. For specific steps, see the following procedures.

To enable certificate authentication in Trust Protection Platform for API users

1. From the Platform menu bar, click **API** > **Default Settings**.
2. In the **Authentication** section, check the box for **Certificate**.

   Fields specific for certificate authentication are shown.
3. In the **Location** field, select field on the X.509 certificate you want to use for matching users with your system's unique identities.
4. In the **Trusted certificate authorities** field, select which CA(s) you want to use as trusted root CAs for issuing client certificates for authentication.

   Use the check boxes to select multiple CAs if needed.
5. Click **Save**.

Now that Trust Protection Platform is configured to allow API users to authenticate with certificates, you need to configure some settings in IIS.

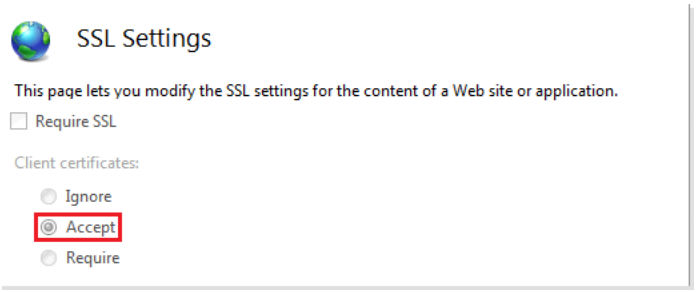
To configure IIS Manager to accept certificate authentication for Remote API access

The VEDAuth server manages certificate authentication for remote Web SDK clients. Even though VEDAuth challenges the client for a certificate, IIS still requires anonymous authentication.

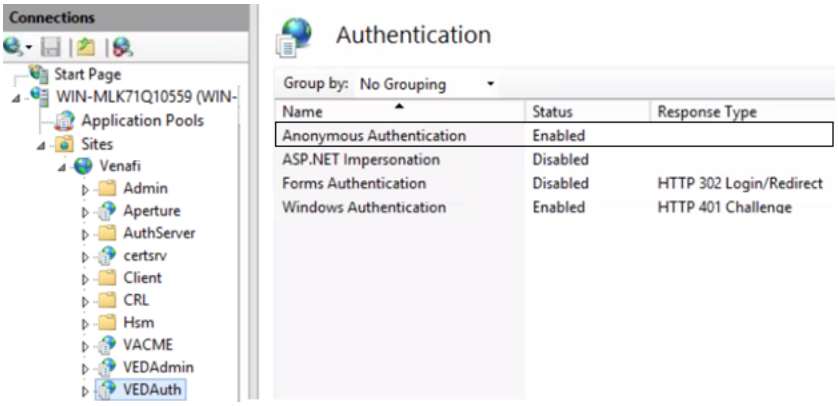
The VEDAuth server can manage both Username/Password and Certificate Authentication. However, do not mix these methods of authentication with Windows Authentication.

1. Open **Server Manager** on the Venafi server.
2. Click **Tools**.
3. Click **Internet Information Services (IIS) Manager**.
4. Navigate to **Sites** > **Venafi** > **VEDAuth**.
5. Click **SSL Settings**.

6. Under **Client Certificates**, specify how to process authentication methods such as Username & Password, Integrated Windows Authentication, or Certificate:
   - **Accept**: Trust Protection Platform Authentication Server allows multiple authentication methods.
   - **Require**: Trust Protection Platform Authentication Server allows only certificate authentication.



7. Click **Apply**.
8. On the VEDAuth web site, click **Authentication**, and then enable **Anonymous Authentication**. For multiple authentication methods, enable **Windows Authentication**.



9. Configure additional certificate authentication settings as necessary. For more information, see Setting up for OAuth token authentication in the *Developer's Guide*.

About Integrated MS Windows Authentication

Integrated MS Windows Authentication allows a browser to prompt the user for credentials. Trust Protection Platform uses those credentials to log in to its web console. It's possible to configure the user's browser to not prompt for credentials and to instead use the credentials of the Windows user that is logged

in to the web consoles.

You can use Windows Integrated Authentication when the web console runs on a Windows Server that is part of a Microsoft Active Directory Domain.

Limitations

- Trust Protection Platform must be a member of your Windows domain.
- Windows Authentication is not compatible with LDAP or local drivers.

"Setting up Windows Integrated Authentication for the web console" below

Setting up Windows Integrated Authentication for the web console

You can use Windows authentication when your IIS server runs on a corporate network that is using Microsoft Active Directory service domain identities or other Windows accounts to identify users.

Prerequisites

- Active Directory Identity Connector should be set up in Venafi Configuration Console.

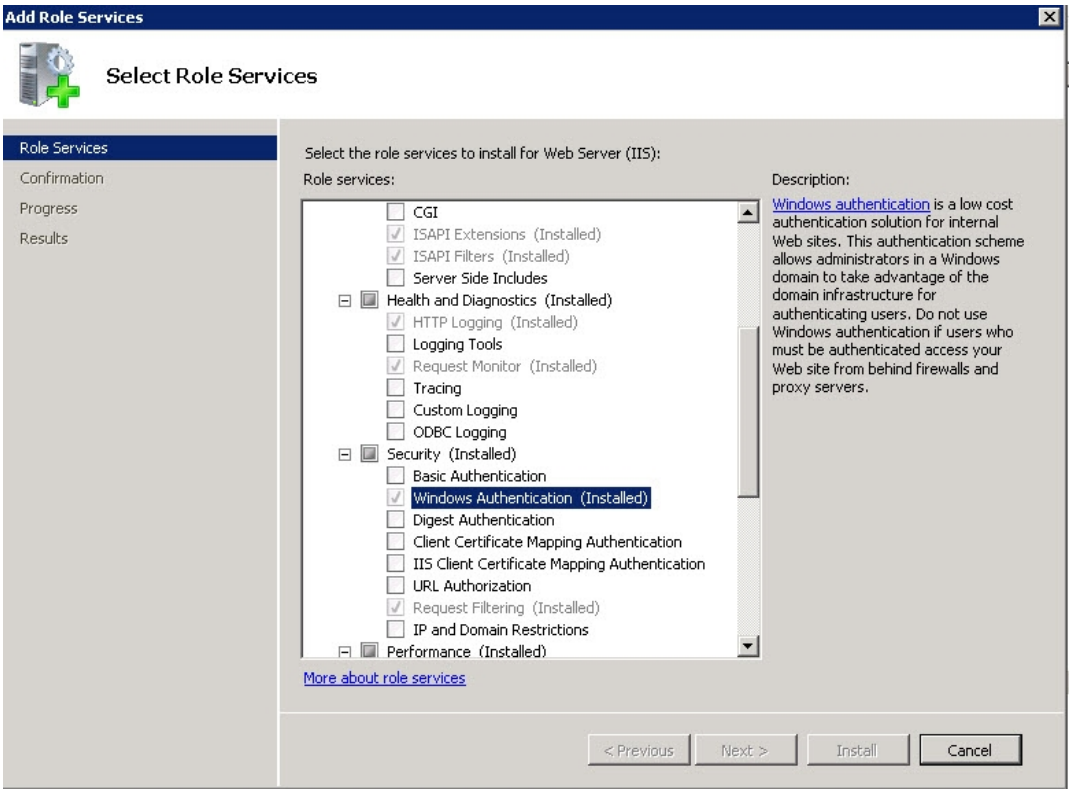
  For more information, see "Creating an Active Directory connection" on page 638 in the *Venafi Trust Protection Platform Administration Guide*.

- The Windows server that Trust Protection Platform is installed on and hosts the Web Console needs to be a member of the Active Directory Forest that you want to support for Windows Integrated Authentication.
- Windows Authentication must be installed as a *role service* of the *web server role* on the Windows machine.

To install Windows Integrated Authentication role services

1. In Windows, click **Start**, and then click **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, click the **Manage** menu, and then click **Add Roles and Features**.
3. In the Add Roles and Features wizard, click **Next**.
4. Select the installation type and click **Next**.
5. Select the destination server and click **Next**.

6. On the Server Roles page, expand **Web Server (IIS)**, expand **Web Server**, expand **Security**, and then select **Windows Authentication**.

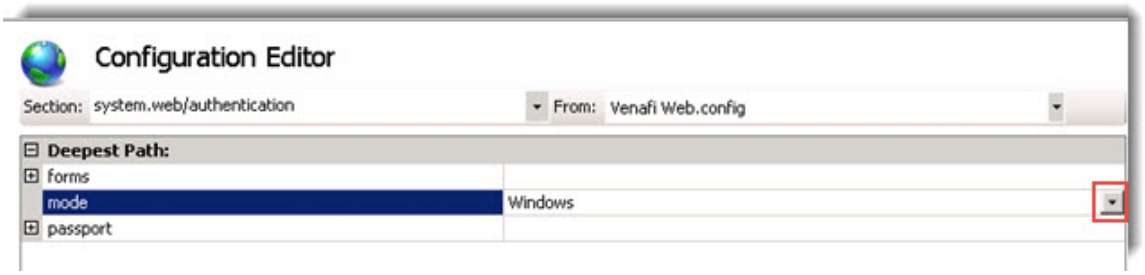


7. Click **Next**.
8. On the Select features page, click **Next**.
9. On the Confirm installation selections page, click **Install**.
10. On the Results page, click **Close**.

To change the authentication mode to Windows

1. Open the Internet Information Services (IIS) Manager.
2. In the **Connections** pane, navigate to the **Venafi** server.
3. Select the console you want to configure (VEDAdmin, VEDAuth, or Aperture)
4. Under **Management**, click **Configuration Editor**.

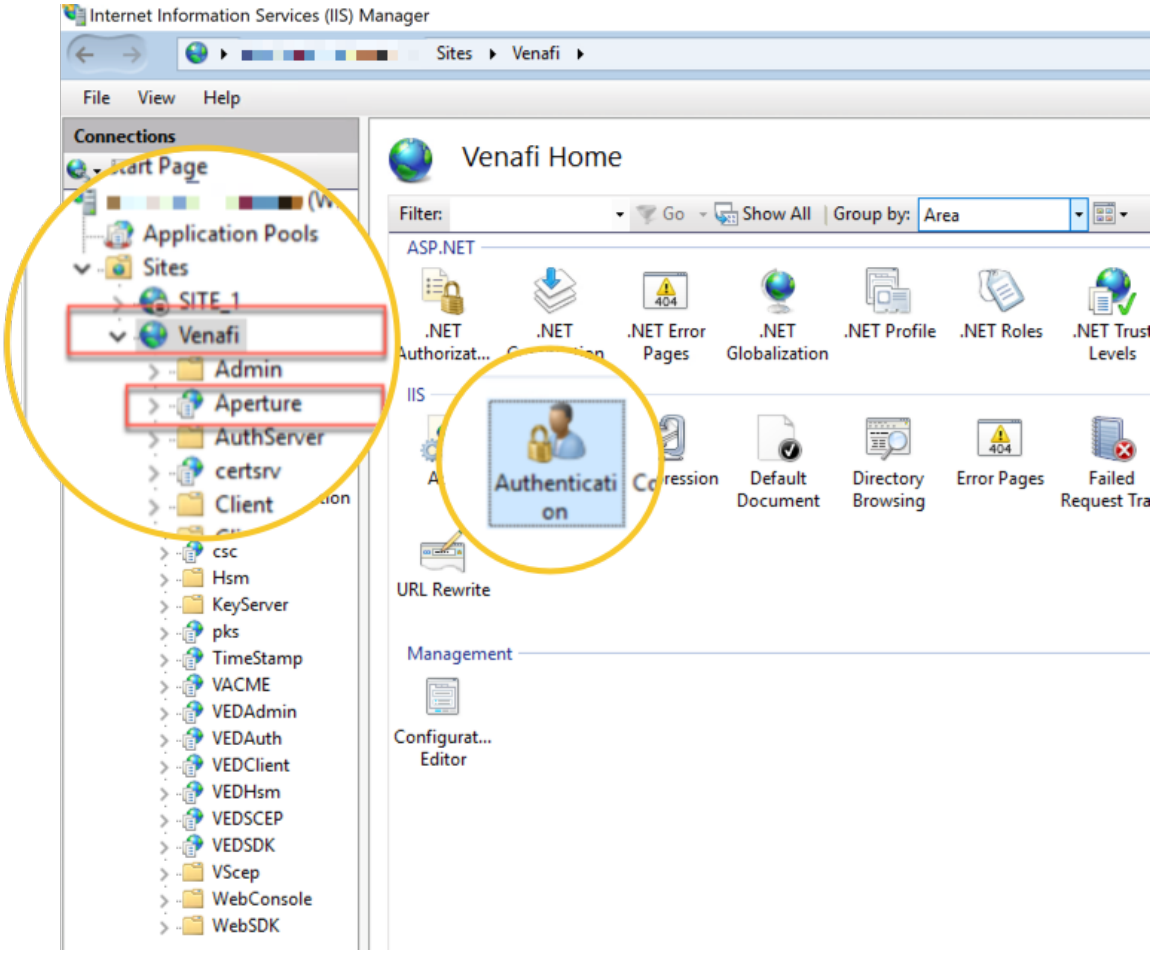
5. In the Configuration Editor Window, in the **Section** drop-down, make sure **system.web/authentication** is selected.
6. In the **Deepest Path** group, **Forms** node, **mode** entry, use the drop-down to change the mode from None to **Windows**.



7. Click **Apply**.
8. Repeat until this process has been done for both VEDAdmin, VEDAuth, and Aperture.

Enabling Windows authentication for Trust Protection Platform

1. Open the Internet Information Services (IIS) Manager.
2. In the **Connections** pane, navigate to the **Venafi** server.
3. Under IIS, click **Authentication**.
4. You will need to modify two sites: **Venafi**, and **Aperture**. For each of the highlighted sites:
    - Right click Anonymous Authentication and choose **Disabled**.
    - Right click Windows Authentication and choose **Enabled**.


Internet Information Services (IIS) Manager
Sites ▸ Venafi ▸
File View Help
Connections
Application Pools
Sites
SITE_1
Venafi
Admin
Aperture
AuthServer
certsrv
Client
csc
Hsm
KeyServer
pks
TimeStamp
VACME
VEDAdmin
VEDAuth
VEDClient
VEDHsm
VEDSCEP
VEDSDK
VScep
WebConsole
WebSDK
Venafi Home
Filter:
Go
Show All
Group by:
Area
ASP.NET
.NET Authorizat...
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
IIS
Authenticati on
Default Document
Directory Browsing
Error Pages
Failed Request Tra
URL Rewrite
Management
Configurat... Editor

For example:


Internet Information Services (IIS) Manager
UX-TPP-1 ▸ Sites ▸ Venafi ▸
File View Help
Connections
Start Page
UX-TPP-1 (UX-TPP-1\Administrator)
Application Pools
Sites
Venafi
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Disabled
ASP.NET Impersonation
Disabled
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Windows Authentication
Enabled
HTTP 401 Challenge

IMPORTANT Be sure to restart IIS after setup.

To configure a user's Windows machine and their web browser for automatic login

NOTE This step is not necessary if you are only configuring Venafi Platform to enable the MMC Snap-In Collection.

First, you need to configure your machine's internet options to allow it to use your username and password for integrated authentication.

1. On the user's local **Windows Control Panel**, open **Internet Options**.
2. Click the **Security** tab, then click **Trusted sites**, then click the **Sites** button.
3. Enter the FQDN for your Trust Protection Platform server, then click **Add**. If you are using a load balancer, enter the FQDN to connect to the cluster, then click **Add**. For example:

   `https://venafi-server.example.com`
4. Click **Close**.

   You'll return to the Security tab.
5. Click **Local intranet**, then click the **Custom Level...** button.
6. Scroll to the bottom of the **Settings** list.
7. Under **User Authentication** > **Logon**, click **Automatic logon with current user name and password**, then click **OK**.
8. Click **OK** on the confirmation window.

   You'll return to the Security tab.
9. Click **Trusted sites**, then click the **Custom Level...** button.
10. Scroll to the bottom of the **Settings** list.
11. Under **User Authentication** > **Logon**, click **Automatic logon with current user name and password**, then click **OK**.
12. Click **OK** on the confirmation window.

You'll return to the Security tab.

13. Click **OK** to save the configuration changes and close the **Properties** window.

Now configure your web browser for automatic login.

1. For Edge, Google Chrome (and other Chromium browsers), see https://sites.google.com/a/chromium.org/dev/developers/design-documents/http-authentication.
2. For Firefox, see https://support.mozilla.org/en-US/kb/Firefox.

Enabling RSA SecurID

Venafi Trust Protection Platform™ supports Windows Integrated Authentication. Trust Protection Platform is also compatible with RSA SecurID and works with the RSA Web Agent for IIS 7. For questions about how to set up and configure the RSA Web Agent for IIS7, please contact RSA SecurID support at http://www.emc.com/support/rsa/index.htm. For your convenience, instructions on how to configure RSA Web Agent and IIS are outlined below.

These instructions apply to Policy Tree and Aperture.

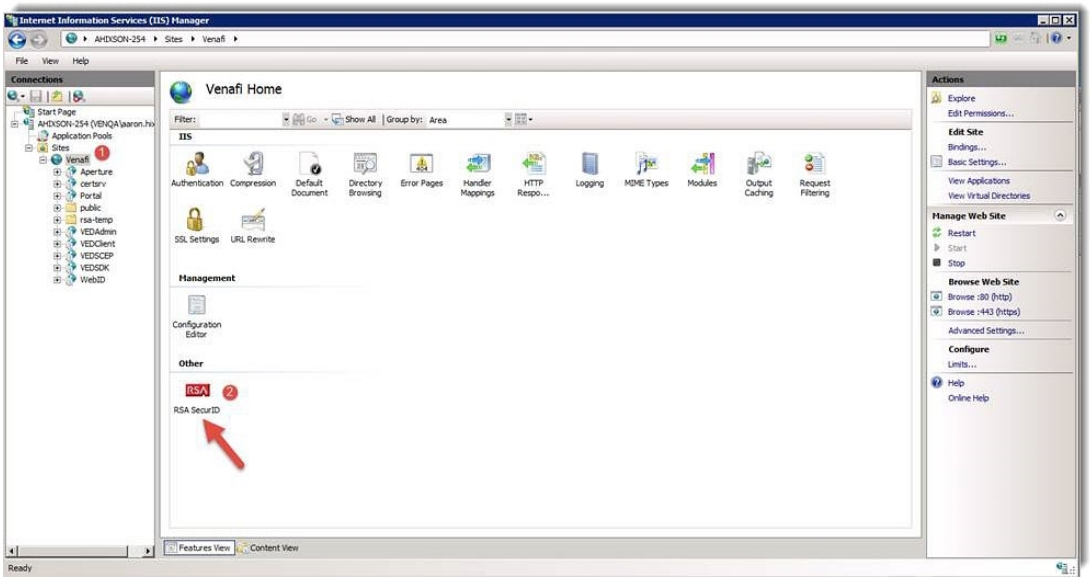
IMPORTANT Because this is an integration with a third party product, single sign-on (SSO) must be enabled and all steps should be followed in their entirety.

To enable RSA SecurID

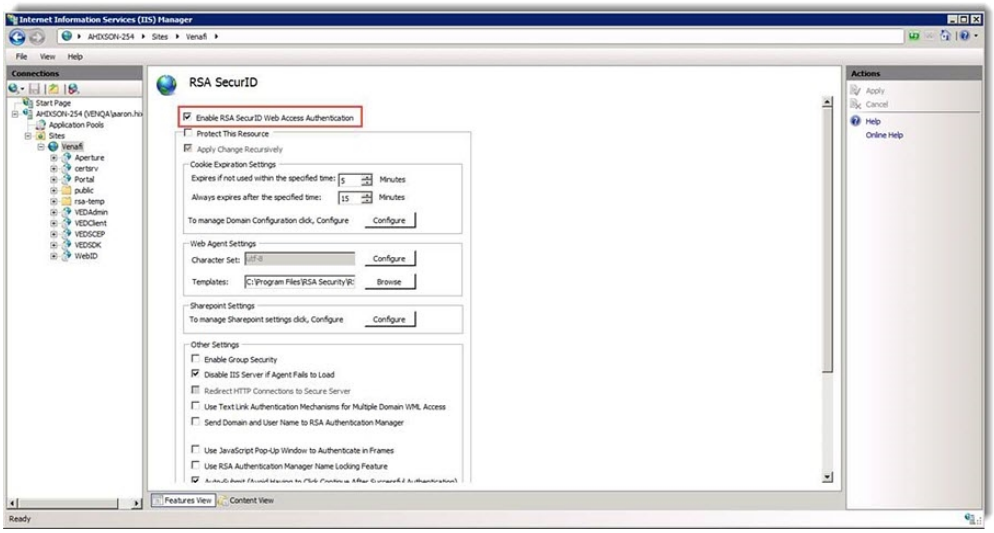
NOTE You may have to refer to RSA's documentation in order to validate and complete some of these steps.

1. Be sure that Windows Authentication has been set up. See "Setting up Windows Integrated Authentication for the web console" on page 797 in the *Venafi Trust Protection Platform Installation Guide*.
2. Get the RSA Agent Configuration file from the administrator of the RSA Authentication Security Manager. The file's name is `AM_Config.zip`.
3. Extract the `sdconf.rec` file from `AM_Config.zip` and place it in C:\Windows\system32.
4. Install the RSA Web Agent on your machine. When prompted, point to the sdconf.rec file during the agent installation.

5. After the installation is complete, open the IIS Management Console.
6. Navigate to the **Venafi** site and under **Other** , click **RSA SecurID**.

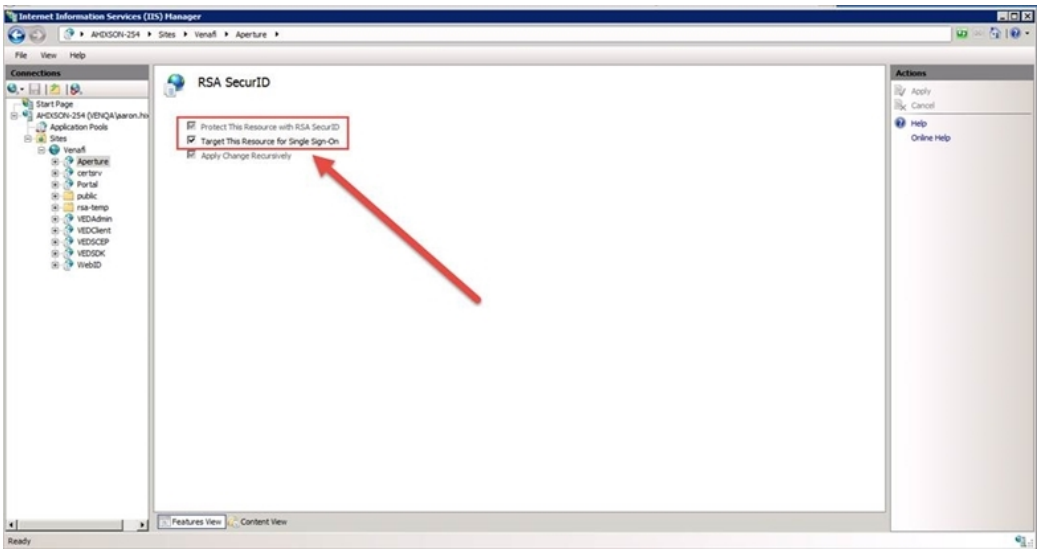


7. Select **Enable RSA SecurID Web Access Authentication** then click **Apply**. Leave all other settings at their defaults.



8. In the **Connections** pane, navigate to and click **Aperture**.
9. Click RSA SecurID,then select **Protect This Resource with RSA SecurID**.

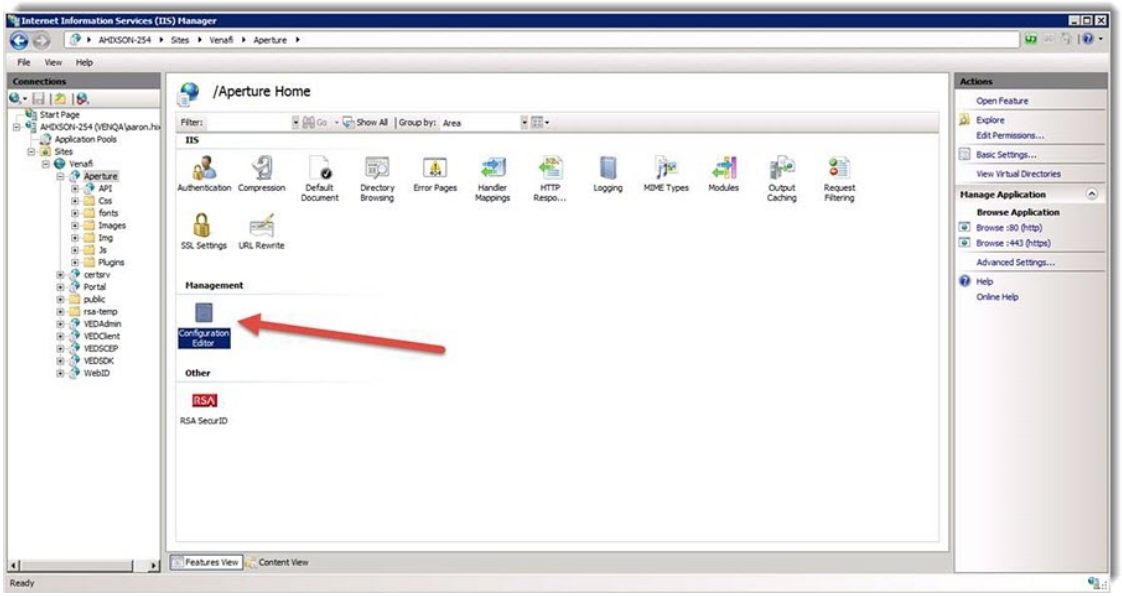
10. Select **Target This Resource for Single Sign-On**.



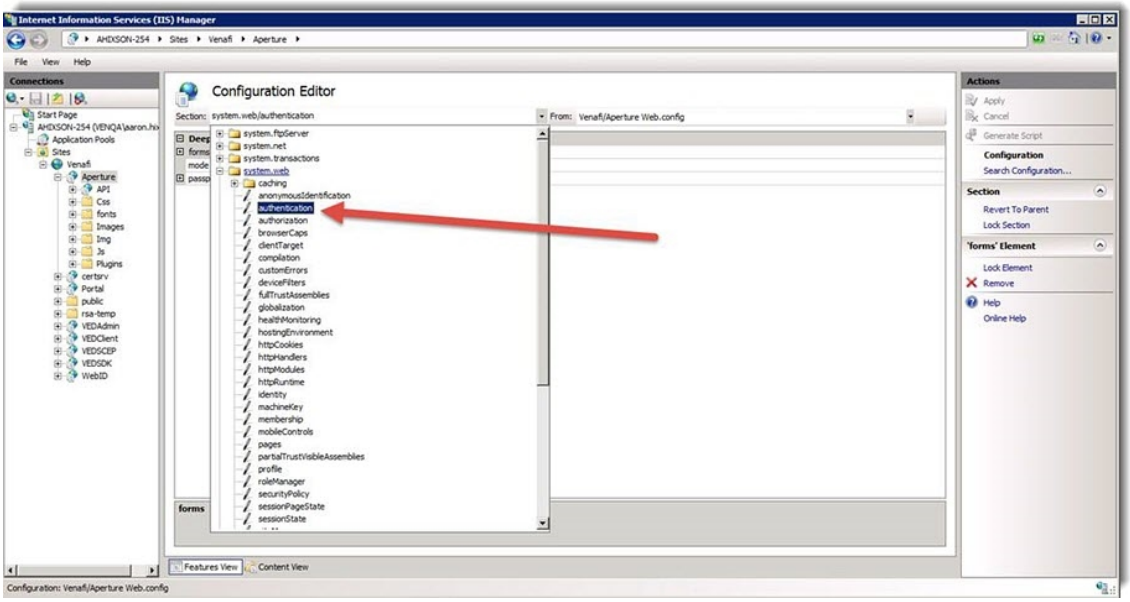
11. Click **Apply**.
12. Repeat Steps 9-11 for the Policy Tree site.

To set the authentication mode

1. In the **Connections** pane, navigate to and click **Aperture**.
2. Under **Management**, click **Configuration Editor**.

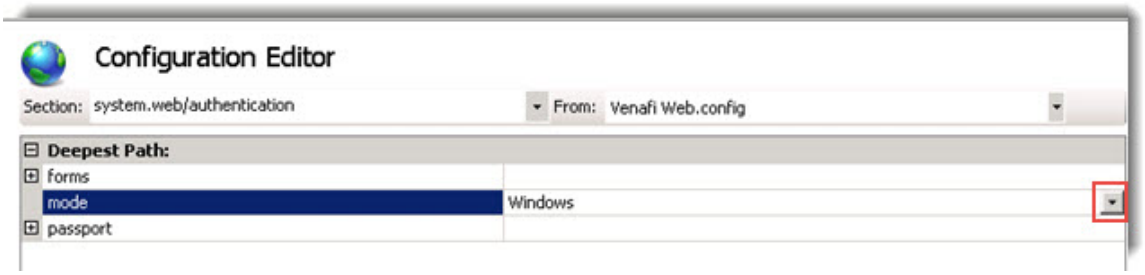


3. Under **Section**, select **system.web** and then select **authentication**.



4. Using the drop-down arrow. change **mode** from none to **Windows**.

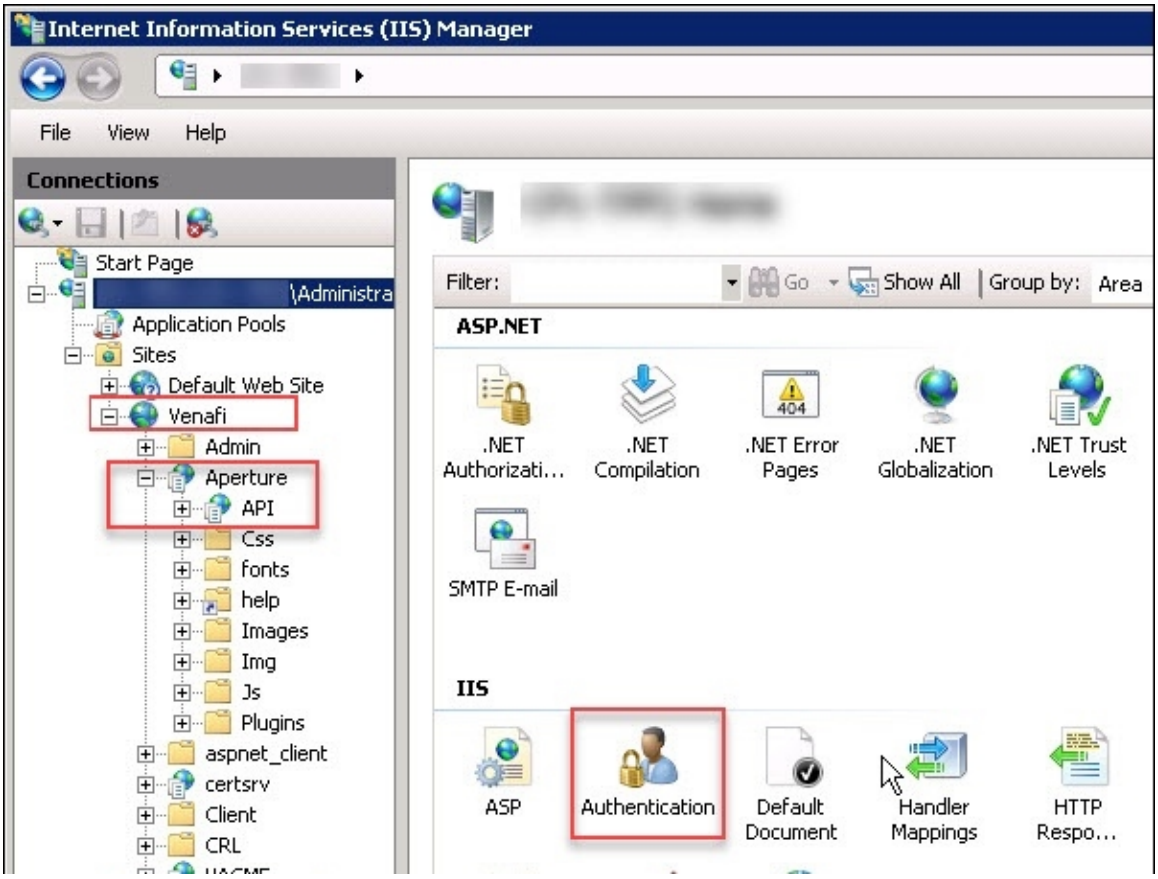
5. Click **Apply**.



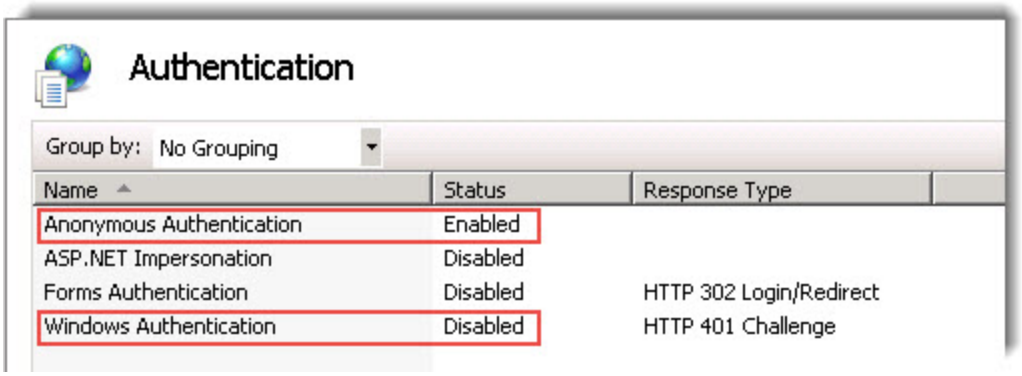
6. Repeat these steps for Policy Tree.

To disable the Windows Authentication login prompt

1. Open the Internet Information Services (IIS) Manager.
2. In the **Connections** pane, navigate to the **Venafi** server, then select **VedAdmin**.
3. Under IIS, click **Authentication**.

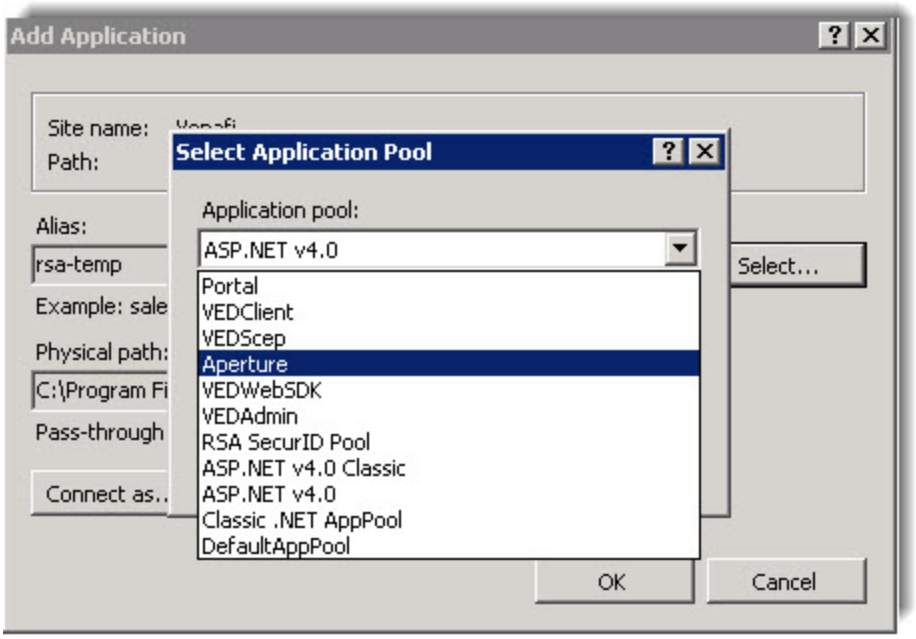


4. Right click Anonymous Authentication and choose **Enabled**.
5. Right click Windows Authentication and choose **Disabled**.



To enable RSA login after a time out

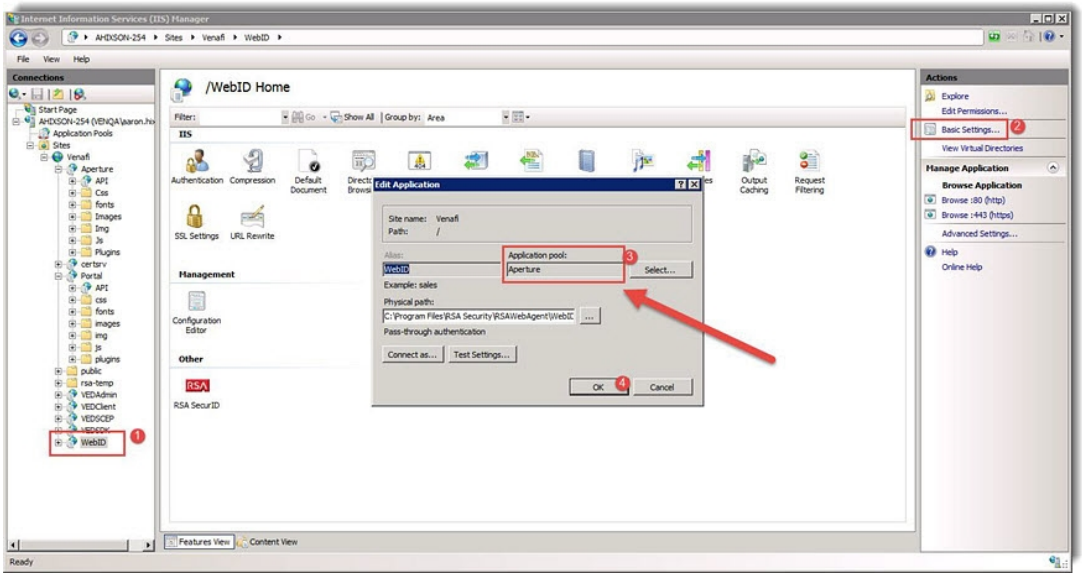
1. In the **Connections** pane, on your server, navigate to **Sites** > **Venafi** > **rsa-temp**.
2. Right-click the **rsa-temp** folder and select **Convert to Application**.
3. In **Add Application**, click **Select**.
4. In **Select Application Pool**, choose **Aperture**.



5. When you're done, click **OK**.

To finish up

1. In the **Connections** pane, navigate to and click **WebID**.
2. Click **Basic Settings...**
3. Change the **Application Pool** to **Aperture**.
4. Click **OK**.
5. Repeat Steps 1-4 for **WebAdmin**.



Users can now access Venafi Platform with their RSA SecurID token.

If you need support from RSA, visit http://www.emc.com/security/rsa-securid/rsa-authentication-agents/iis-7-1.htm.

Oracle Access Manager settings

Enables *single sign-on* (SSO) authentication via Oracle Access Manager v10.1.

> **NOTE** SAML SSO authentication is supported by Oracle Access Manager. For more information, see "Working with SAML for single sign-on (SSO)" on the next page.

Prerequisites for Configuration

- Oracle Access Manager WebGate version 7.0.4 or 10.1.4.0 must be installed on the Trust Protection Platform server.
- If you are using Oracle Access Manager WebGate version 10.1.4.0, you must install the Oracle Access Manager 10.1.4.2 WebGate Patch.
- Trust Protection Platform must have a connection to an external user datastore.
- The Active Directory connection must have the Oracle Access Manager schema extension.

- The user account Trust Protection Platform uses to connect to the external user datastore must have permissions to read the User or Group information for any user who attempts to log in to Policy Tree.

System requirements for Oracle Access Manager

To support Oracle Access Manager single sign-on for the Trust Protection Platform's Policy Tree and Aperture:

- Oracle Access Manager WebGate version 7.0.4 or 10.1.4.0 must be installed on the Trust Protection Platform server.
- If you are using Oracle Access Manager WebGate version 10.1.4.0, you must install the Oracle Access Manager 10.1.4.2 WebGate Patch.
- Trust Protection Platform must have a connection to an external user datastore.

  For more information, see "Creating an Active Directory connection" on page 638.
- The Active Directory connection must have the Oracle Access Manager schema extension.
- The user account Trust Protection Platform uses to connect to the external user datastore must have permissions to read the User or Group information for any user who attempts to log in to Policy Tree.

  The user account used to connect to Active Directory is defined in the Directory Connection object. For more information, see "Creating an Active Directory connection" on page 638.

Working with SAML for single sign-on (SSO)

Venafi Platform allows you to use modern single sign-on (SSO) identity providers (like Okta, Azure, Ping Identity, etc.) that use the SAML 2.0 standard. Using a third-party identity provider can greatly enhance your security posture. For example, they can simplify configuration of two-factor authentication (2FA), a protection against phishing threats and other password vulnerabilities.

Venafi Platform has long allowed you to use a variety of single sign-on methods like Windows authentication and certificate authentication. With the ability to connect to identity providers (IDP) via SAML, you have even more options for protecting your machine identity management system.

In this release of Venafi Platform, there are some items you should be aware of:

- When you import the identity provider SAML file, the associated certificate is automatically enrolled in TLS Protect at the *monitoring* level. A higher level of enrollment is not possible, since SAML certificates are not issued and imported like a normal certificate. To renew the

SAML certificate you need an entirely new identity provider metadata file.

- Venafi Platform requires the entire SAML Response to be signed (but not encrypted, which is not supported). Some IDPs only sign the Assertion, so you may need to specify signing the entire Response.
- We do not support signed authentication requests.
- The default search expression will need to be changed, as documented in the phase one instructions.
- We do not currently support single log out (SLO), however, we do support a Logout URL, if your IDP allows you to log out by simply visiting a URL.
- We do not support forced log on.
- You can only configure one Authentication connector at a time. We don't support multiple connectors.
- While any SAML 2.0 IDP should work, we have tested with the following:
  - Active Directory
  - Azure
  - Okta
  - Ping
- The clock skew allowance is set to 180 seconds. The Venafi server and IDP server time can be off by 180 seconds and still sign in.

Configuration process

There are three high-level steps to configure SAML SSO for Venafi Platform.



Phase 1. Prepare Venafi Platform for SAML and obtain the Service Provider Metadata XML file. See the steps in "Prepare Venafi Platform for SAML SSO" on page 813.

Phase 2. Configure the Identity Provider and obtain the IDP Metadata XML file. The steps for phase two depend on your IDP. We've tested and outlined the following:

- ADFS
- Azure
- Okta
- Ping Federate
- Ping One

Phase 3. Configure SAML on your Venafi server. See the steps in "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

If you have questions, try reviewing "SAML troubleshooting tips" on page 835.

Technical implementation details

On the SAML signing certificate we verify:

- The certificate is not expired
- The certificate matches the certificate we have on file for the SAML profile
- The correct certificate was used to create the signature
- The signature is still valid (validity period hasn't expired and certificate has not been revoked).

The SAML Response must:

- Contain the `ID` attribute
- Contain the `version` attribute, and the version must be `2.0`
- The `InResponseTo` attribute must match TPP's authentication flow
- Have a signature on the response
- The `destination` must be entered, and must match the FQDN of the Venafi cluster
- `Status` must be present, and have a value of `Success`
- `Issuer` must be present, and must match the issuer on the SAML profile

The SAML Assertion must:

- Contain the `version` attribute, and the version must be `2.0`
- `Audience` attribute must equal the Venafi Platform service provider ID

- Contain a `Subject`
- `SubjectConfirmation` attribute must be present, and have the method of `bearer`
- If the assertion is signed, the signature must be valid (however, the assertion does not need to be signed)
- The `NotBefore` and `NotAfter` attributes in the Conditions are validated, respecting clock skew
- Contain the `Issuer`, which must match the issuer on the SAML profile
- Assertion `ID` must be present
- The `NotOnOrAfter` attribute must be present in the assertion

Prepare Venafi Platform for SAML SSO

Venafi Platform supports a number of popular SAML single sign-on (SSO) identity providers for modern SSO user authentication.

Configuring SAML single sign-on (SSO) is a multi-step process that involves getting your Venafi instance ready, configuring your identity provider, and then incorporating your identity provider's data in Venafi Configuration Console.

This topic is part of Phase One (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

Phase One of SAML SSO configuration can be broken down into the following processes:

1. Configure your FQDN in Venafi Platform's Platform tree so it knows what URL people are using to access its services. This is required because the signed SAML Response is linked to the FQDN, and if this isn't configured properly, SSO won't work.
2. Ensure you have an LDAP or Active Directory (AD) connection to an identity directory that is connected to your SAML Identity Provider (IDP).
3. Configure the User Search Expression for you identity store (LDAP or AD). This step uniquely links users in your directory with users in Venafi Platform via a specific user identifier, like UPN.
4. Export your Venafi Service Provider Metadata XML file. This file (or the data it contains) will be required for phase two: configuring your IDP.

Each of these processes is described in the sections below.

Phase 1.1: Configure your FQDN

A secure SAML SSO process requires you provide the FQND (fully-qualified domain name) users enter to access Venafi Platform. Most organizations use multiple Venafi Platform servers to provide redundancy and load balancing. The server doesn't know the URL (of, for example, the load balancer) but the FQDN is required for secure communication between your Venafi server and the IDP. Use the following procedure to configure your FQDN in the web console.

To configure your FQDN in Venafi Platform

1. From the Platform menu bar, click Policy Tree.
2. Click the **Platforms** tree.

   You will be taken to the **Platforms** root, **Platforms** tab.
3. Click the **Engine** sub-tab.
4. In Trust Protection Platform **URL HostNames**, locate **Aperture (/Aperture)**, and enter the FQDN or IP address used to access Venafi Platform. The value you enter should match the FQDN found in the common name or DNS Subject Alternative Name of your CA-issued Venafi Operational Certificate so users don't encounter a certificate error.

   > **NOTE** Do NOT include the protocol (`https://`), or the `/Aperture` directory. Just enter the FQDN itself. So, if your Aperture URL is `https://platform.venafi.com/Aperture`, you would enter:
   >
   > ```
   > platform.venafi.com
   > ```
5. Click **Save**.

Phase 1.2: Ensure you have connected Venafi Platform to AD or LDAP

In Venafi Platform version 25.1, there is no support for just-in-time account creation, so you need to have Venafi Platform accounts for all users who will be logging in via the SAML identity provider as Active Directory (AD) or LDAP users.

It is important that your users are queryable by the value put in the NameID parameter of the Subject section of the SAML assertion. For example:

- For AD users, if the SAML IDP is using the e-mail address of the authenticated user as the NameID, then the Venafi Platform AD identity provider User Search properties should be configured to customize the user lookup to the email address. For details on customizing the user

lookup to the email address, see "Phase 1.3: Configure SAML user search expression" below.

- For LDAP users, if the SAML IDP is using the UPN (User Principle Name) of the authenticated user as the `NameID`, then the Venafi Platform LDAP identity driver User Search properties should be configured to add `userPrincipalName` (or whatever the corresponding attribute is in your LDAP directory) as described in "Phase 1.3: Configure SAML user search expression" below.

  Whatever the attribute is, you want to follow these guidelines:

  - The attribute is something that the SAML IDP can provide.
  - The attribute is something that Venafi Platform has access to and can query against.
  - The attribute uniquely identifies one (and only one) user. If more than one user is returned in the query, authentication will fail an ambiguity security check.

Regardless of the identity provider, you need to export Venafi Platform data that you will use to connect to the identity provider.

The steps you need to take to configure Active Directory are in "Creating an Active Directory connection" on page 638. Complete AD configuration information can be found in "Working with Active Directory" on page 636

The steps you need to take to configure LDAP are in "Creating an LDAP connection" on page 650. Complete LDAP configuration information can be found in "Working with LDAP and Oracle directory service" on page 648.

Phase 1.3: Configure SAML user search expression

When configuring a SAML-based identity provider configuration for logging in to Venafi Platform, you need to ensure the identity driver is configured to customize the user lookup to correctly and uniquely identify users.

You need to work with your identity management team to determine what type of unique identifier you are able to pass into the user assertion. We recommend using UPN, but you can use any unique attribute that is available to be put as the `Name ID` of the SAML assertion, and is available for query via your AD or LDAP connection.

To customize the user lookup in Venafi Configuration Console

1. Use Remote Desktop to connect to the Venafi Platform host machine, and open the **Venafi Configuration Console**.

2. Click the **Connectors** node.
3. Click the identity connector used by Active Directory.
4. In the actions panel, click **Properties**.
5. [Conditional] If necessary, log in to Venafi Platform as a master administrator.

   The next step depends on whether you are connecting with AD or LDAP.

For Active Directory

a. Click the **User Search** tab.

b. Click **Use Custom Expression**.

c. Change the value from:

```
(&(ANR=$search$*)(objectCategory=$userclass$))
```

to:

```
(&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))
```

Unless your IDP is *not* sending the UPN of the user within the `userID`, in which case you should enter the following to search by e-mail address:

```
(&(|(ANR=$search$)(mail=$search$))(objectCategory=$userclass$))
```

> **TIP** Since this string uses the e-mail address of the user, and since an email address may not be unique in some systems, this is not the preferred option.

d. Click **OK**.

e. Open a command window, and reset IIS using the following command:

```
iisreset
```

For LDAP

a. Click the **Search Resolution** tab.

b. From **Available Attributes**, add both the following: `ANR`, and `userPrincipalName`.

c. Click **Add**.

d. Click **OK** to save.

e. Open a command window, and reset IIS using the following command:

```
iisreset
```

6. Log in to Aperture, and find an identity field, and verify that you can find one (and only one) user, searching with sample data that will be put in the `Name ID` of the SAML assertions.

   For example, if you're using UPN with Active Directory, log in as an AD user, and in a contact field search for a known email address in your organization (e.g. jane.doe@venafi.com) to make sure that one, and only one result is returned.

Now that you have configured the user lookup search expression, you're ready to move on to retrieving your Service Provider Metadata XML file.

Phase 1.4: retrieve Venafi Platform service Provider Metadata XML

In SAML authentication, the service provider (in this case Venafi Platform) publishes an XML metadata file, which is used for making the connection between the service provider and the identity provider. You need to export that file from Venafi Configuration Console using the following procedure.

To retrieve the service provider metadata XML file

1. Use Remote Desktop to connect to your Venafi server, and open Venafi Configuration Console.
2. Click the **Authentication** node.
3. Click the **SAML** component.
4. In the **Actions** panel, click **Properties**.
5. [Conditional] If requested, enter a master administrator username and password for Venafi Platform.
6. Select your **IdP Vendor** from the drop-down list.

The settings window will populate based on your selection with the specific fields and terms for your identity provider.

If you are using a non-tested IdP vendor, select **Other**, then enter the IdP name. This name will be used to identify the SAML configuration and for placing the certificate in the policy tree.

7. [Optional] Configure the **Default Return URL**. This is the default URL users will be taken to upon successful login through the SAML provider. Most organizations use `aperture`, as that is the most common starting place for users of the platform.

8. [Optional] Configure the **Log out URL**. If supported by your IdP, this is the URL that will trigger a log out of a session. As far as we know, Azure is the only tested IdP that supports a log-out URL.

   If your IdP does not support a Log out URL, and nothing is entered in this field, then Venafi Platform will not have a log-out option in the menu. After configuring this setting you need to restart IIS before you will see the change in the menu.

9. In the **Export and import SAML metadata** section, click **Export service provider file** and save the file to a location you'll be able to access during Phase 2.
   - Most identity providers can import the SP metadata XML file directly.
   - If your identity provider (including Okta) cannot import the SP metadata XML file, refer to the **Service provider details** for the URLs you will need when configuring your identity provider.

What's next?

When you've completed all four steps in phase one, you're ready to move on to phase two where you will configure your IDP.

While you *should* be able to connect Venafi Platform with any IDP that supports the SAML 2.0 standard, Venafi has tested and is providing guidance on using the following identity providers:

- "How to configure ADFS for SSO" on the facing page
- "How to configure Azure for SSO" on page 822
- "How to configure Okta for SSO" on page 824
- "How to configure PingFederate for SSO" on page 826
- "How to configure PingOne for Enterprise for SSO" on page 831

NOTE Venafi Platform 25.1 only supports a single identity provider connection at a time. Multiple IDP connections may be considered for a future release.

How to configure ADFS for SSO

This topic details how to configure Microsoft Active Directory Federated Services (ADFS) for single sign-on (SSO).

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

ADFS is a common identity provider due to the integration with many organizations' existing identity infrastructure, while supporting SSO to cloud and other SaaS resources, even though ADFS typically sits behind the corporate firewall.

NOTE These setup instructions were written based on Windows Server 2016. If your Windows server is different, there may be minor adjustments you need to make.

You must have an existing functional ADFS deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to ADFS. The application is referred to in ADFS as a "Relaying Party Trust."

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via ADFS. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure ADFS for single sign-on

1. Log in to your ADFS Windows server and launch **AD FS Management** console.
2. In the Action Panel, click **Add Relying Party Trust**.

3. Click **Claims aware**, then click **Start**.
4. Select **Import data about the relying party from a file**.
5. Click **Browse**, and browse to the location where you saved the Service Provider Metadata XML file (done in "Prepare Venafi Platform for SAML SSO" on page 813).
6. Click **Next**.
7. Provide the Application (Relying Party Trust) name, then click **Next**.

   For example, you could enter something like: `Venafi Platform Production`.

   > **TIP** If needed, you may want to differentiate between production, stage, and test environments.

8. Select who within you organization will be able to authenticate to Venafi Platform via ADFS, based on your access control policy and your discussions with your identity team and your machine identity management (or PKI) team, then click **Next**.
9. [Optional] Review, if desired, the data on the tabs on the **Ready to Add Trust** screen. These values were either set by you using the wizard, or were configured automatically from the Service Provider Metadata XML file you imported.
10. Click **Next**.
11. Leave **Configure claims insurance policy for this application** checked, then click **Close**.
12. In the **Edit Claim Insurance Policy** window you configure how ADFS identifies a user within the SAML assertion, and should match exactly the User Search Expression you used for Venafi Platform in "Phase 1.3: Configure SAML user search expression" on page 815.

    For example, if your search expression is `(&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))` then you are expecting a UPN to be specified in the SAML assertion created by ADFS.

    If your search expression is `(&(|(ANR=$search$)(mail=$search$))(objectCategory=$userclass$))` then you are expecting an email address to be specified in the SAML assertion.

    > **TIP** Active Directory does not enforce uniqueness of the email field, so be careful to choose attributes that are guaranteed to uniquely identify a user.

13. Click **Add Rule...**
14. Click Send **LDAP Attributes as Claims**, then click **Next**.

15. On the **Configure Claim Rule tab**, do the following:
    a. Give the rule a descriptive name.
    b. For the **Attribute Store**, select **Active Directory**.
    c. For **LDAP Attribute**, select **User-Principal-Name** (or whatever selection best matches your user search expression.)
    d. For **Outgoing Claim Type**, select **Name ID**.
    e. Click **Finish**.
16. Click your rule in the list, then click **OK**.
17. Open a PowerShell prompt (run as Administrator) on the ADFS server.
18. Enter the following command, replacing '<Name goes here>' with the name you gave your application earlier in the process:

    ```
    Get-AdfsRelyingPartyTrust -Name '<Name goes here>' |Set-AdfsRelyingPartyTrust -SamlResponseSign MessageAndAssertion
    ```

    For example, if you used the name from our example, you would use the following PowerShell command:

    ```
    Get-AdfsRelyingPartyTrust -Name 'Venafi Platform Production' |Set-AdfsRelyingPartyTrust -SamlResponseSign MessageAndAssertion
    ```

    This command sets an option that is not exposed in the ADFS UI to sign all SAML responses, which is a requirement of Venafi Platform.
19. From your ADFS server, open a web browser and visit:

    https://localhost/federationmetadata/2007-06/federationmetadata.xml

    We refer to this file as the *IDP Metadata XML file* in our documentation.
20. Download the federationmetadata.xml file to your Venafi Platform server as an XML file.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure Azure for SSO

This topic details how to configure Microsoft Azure for single sign-on (SSO). Azure is a cloud computing service used for building, testing, deploying, and managing applications through Microsoft-managed data centers.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional Azure deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to Azure.

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Azure. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure Azure for single sign-on

1. Log in to the Azure portal and go to **Enterprise Applications**.
2. Click **+ New application**.
3. Switch to the **old app gallery experience**.
4. Click **Non-gallery application**.
5. Enter a name for the Venafi Platform cluster you are integrating with, then click **Add**.

   This process may take a minute or more without a visual sign of progress, so be patient.

6. From the new application Overview page browse to **Manage** > **Users and Groups**, and click **+ Add user**.
7. In **Add Assignment**, click the **Users and Groups** bar to pull out a Users and Group list.
8. Enter the search pattern for the new group or user, select the new user from the results, and click **Select**.

   You'll be taken back to **Add Assignment**, where you will see a count of users selected.
9. Click **Assign** to complete the assignment
10. Click **Manage** > **Single sign-on** and select **SAML** as the single sign-on method.

    You'll see the **SAML-based Sign-on** page.
11. Click **Upload metadata file**.

    For the next step, you'll need the Service Provider Metadata XML file.
12. Browse to the Service Provider Metadata XML file you exported from Venafi Platform and click **Add**.

    You will see the contents of the XML file in the **Basic SAML Configuration** panel.
13. Click **Save**.
14. Close the panel and click **No, I'll test it later**.
15. In **User Attributes & Claims**, click **Edit**.
16. In **SAML Signing Certificate > Signing Option** select **Sign SAML response**, and click **Save**.
17. Close the panel and click **No, I'll test it later**.
18. In **SAML Signing Certificate** > **Federation Metadata XML**, click **Download**.

    The IDP Metadata XML file will be downloaded. Save it to a place where you will be able to find it easily.
19. In **Set up <APPLICATION NAME>** copy the **Logout URL** and paste it to a blank text file on the Venafi server.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure Okta for SSO

This topic details how to configure Okta for single sign-on (SSO). Okta is a common identity provider with wide application support.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

> **IMPORTANT** Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional Okta deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to Okta. Consult the Okta documentation if you need to configure Okta to obtain data from your identity store.

Before you begin, you will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Okta. You'll need that information near the end of the procedure below.

> **IMPORTANT** While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure Okta for single sign-on

1. Log in to the Okta Classic UI.
2. From the menu, click **Applications** > **Applications**.
3. Click **Add Application**.
4. Click **Create New App**.

   You should see the **Create a New Application Integration** dialog box.
5. For **Platform**, select **Web**.
6. For **Sign on method**, select **SAML 2.0**.

7. Click **Create**.

   You should see the **Create SAML Integration** page, opened to step 1, **General Settings**.

8. Enter a unique name for the Venafi Platform cluster you are integrating with.

   The name must be unique in your Okta application list.

9. [Optional] Add a logo if desired, then click **Next** (leaving the boxes unchecked).

   You should see step 2, **Configure SAML**.

   Okta does *not* allow you to import the SP Metadata XML file, so for the next step, you will need to copy information from the **SAML Properties** window in Venafi Configuration Console.

10. In General settings:

    a. In **Single sign on URL**, paste the corresponding URL from the **Service provider details** section of the **SAML Properties** window in Venafi Configuration Console.

       For example: `https://test.venafi.com/aperture/api/saml/acs`

    b. Select the box for **Use this for Recipient URL and Destination URL**.

    c. Leave the box *unselected* for **Allow this app to request other SSO URLs**.

    d. In **Audience URI (SP Entity ID)**, paste the corresponding URL from the **Service provider details** section of the **SAML Properties** window in Venafi Configuration Console.

       For example: `https://test.venafi.com/aperture/api/saml/acs`

    e. Leave **Default RelayState** empty.

    f. For **Name ID format**, select **EmailAddress**.

    g. For **Application username**, select **Email**.

11. Click **Show Advanced Settings**, and complete the following fields:

Field	Value
Response	Signed
Assertion Signature	Unsigned
Signature Algorithm	RSA-SHA256

Field	Value
Assertion Encryption	Unencrypted
Enable Single Logout	*Leave unselected*
Authentication Context Class:	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	*Leave blank*

12. Leaving all the rest of the attributes in their default state, scroll to the bottom of the form and click **Next**.

    You will be taken to step 3: **Feedback**.

13. Select **I'm an Okta customer adding an internal app**.

14. Click **Finish**.

    The application integration will be created, and you'll be taken to the application details page.

15. On the **Sign On** tab, under **Settings** > **Sign On Methods**, click **Identity Provider metadata**.

16. Download the IdP Metadata XML file on the Venafi Platform host.

    For example: `Okta-IdP-metadata.xml` (the file name is irrelevant).

    > **TIP** Make sure your text editor does not add any non-text characters to the file.

17. On the **Assignments** tab, click **Assign** > **Assign to people**.

18. For each user you want to be able to access Venafi Platform via SAML, click the **Assign** button next to their name, then click the **Save and Go Back** button.

19. Repeat the last step for each user, then click **Done**.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure PingFederate for SSO

This topic details how to configure PingFederate for single sign-on (SSO).

> **IMPORTANT** Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

PingFederate is an on-premise single sign-on (SSO) identity provider and directory service.

NOTE These instructions were written based on PingFederate 10.2 on Windows Server 2016. If your server or software version is different, you will need to make necessary adjustments.

You must have an existing functional PingFederate deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform).

You will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via Ping Federate. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure PingFederate for single sign-on

1. Log in to PingFederate on-premise, and open **Applications**.
2. From the side menu, click **Integration** > **SP Connections**.
3. Click **Create Connection**.

   PingFederate does not support the Service Provider Metadata XML file, which is why you can't click *Import Connection*.
4. In the SP Connections section:
   a. In the Connection Template tab

Field	Value
Template	Do not use a template for this connection

   b. In the Connection Type tab

Field	Value
Browser SSO Profiles	*Checked*
Protocol	SAML 2.0
WS-Trusts STS	*Unchecked*
Outbound Provisioning	*Unchecked*

Click **Next**.

c. In the Connection Options tab

Field	Value
Browser SSO	*Checked*
Attribute Query	*Unchecked*

Click **Next**.

d. In the Import Metadata tab

Field	Value
Metadata	File (radio button)

Then click **Choose File**, and select the Service Provider Metadata XML file you saved from Venafi Platform, then click **Next**.

e. In the Metadata Summary tab

Field	Value
Entity ID	*This field will contain the FQDN obtained from the XML file.*

Click **Next**.

f. In the General Info tab

Field	Value
Partner's Entity ID	*This field will contain the EntityID from the XML file.*
Connection	*This field will contain the Entity ID from the XML file. You can*

Field	Value
Name	*customize this, if you prefer.*
Base URL	*This field will contain the URL from the XML file.*

Click **Next**.

g. In the Browser SSO tab, click **Configure Browser SSO**.

- In the SAML Profiles sub-tab,
  - *Check* - **IDP-INITIATED SSO** (only works if Venafi Platform is reachable by IP address or FQDN)
  - *Check* - **SP-INITIATED SSO**.
  - *Unchecked* - **IDP-INITIATED SLO**.
  - *Unchecked* - **SP-INITIATED SLO**.
- In the Assertion Lifetime sub-tab, leave default settings.
- In the Assertion Creation sub-tab, click **Configure Assertion Creation**.
  - On Identity Mapping, select **STANDARD**.
  - On Attribute Contract select the following from the **SAML_Subject** dropdown: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - On Authentication Source Mapping, click **Map New Adapter Instance**.
    - For Adapter Instance, select **FederateUsers**.
    - For Mapping Method, select **Use only the Adapter Contract values in the SAML assertion**.
    - For Attribute Contract Fulfillment:

Attribute	Source	Value
SAML_SUBJECT	Adapter	username

    - For Issuance Criteria, leave empty.

- For Summary, review, then click **Done**.

  You'll be taken back to the Authentication Source Mapping page. Click **Next**.

- On Summary, review, then click **Done**.

  You'll be taken back to the Assertion Creation sub-tab. Click **Next**.

- In the Protocol Settings sub-tab, click **Configure Protocol Settings**.
  - On Assertion Customer Service URL, accept the default settings.
  - On Allowable SAML Bindings:

Field	Setting
Artifact	*Unchecked*
Post	*Checked*
Redirect	*Checked*
SOAP	*Unchecked*

  - On Signature Policy:

Field	Setting
Require Authn Requests...	*Unchecked*
Always sign assertion	*Checked*
Sign Response as required	*Checked*

  - On Encryption Policy, accept the default settings (none).
  - On Protocol Settings Summary, review, then click **Done**.

    You'll be taken back to the Protocol Settings page. Click **Next**.

- In the Summary sub-tab, review, then click **Done**.

  You'll be taken back to the Browser SSO tab. Click **Next**.

h. In the Credentials tab, click **Configure Credentials**.

- In the Digital Security Settings sub-tab:

Field	Value
Signing Certificate	*Select any; If none exist, click Manage Certificates to either create one or import one for use.*
Signing Algorithm	RSA SHA256

- In the Summary sub-tab, review, then click **Done**.

  You'll be taken back to the Credentials tab. Click **Next**.

i. In the Activation and Summary tab, review your selections, then click **Save**.

   You'll be taken back to the SP Connections section, where you can see the newly-created connection.

5. In the SP Connections section, locate your newly-created connection, then click **Select Action** > **Export Metadata**.
6. On the Metadata Signing sub-tab, select any signing certificate, and select the **RSA SHA256** signing algorithm, then click **Next**.
7. On the Export & Sumary sub-tab, click **Export**. We refer to this file as the *IDP Metadata XML file* in our documentation.

   You'll need to save this to your Venafi Platform server, in a place you can find it later.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on page 834.

How to configure PingOne for Enterprise for SSO

This topic details how to configure PingOne for Enterprise single sign-on (SSO). PingOne for Enterprise is a cloud-based authentication provider.

This topic is part of Phase Two (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

IMPORTANT Before completing these steps, you will need to follow the steps in "Prepare Venafi Platform for SAML SSO" on page 813. You will need configuration information from the Venafi Service Provider Metadata XML file to complete this process.

You must have an existing functional PingOne for Enterprise deployment to use these steps. These instructions detail how to add a new Application (Venafi Platform) to PingOne. Consult the PingOne for Enterprise documentation if you need to configure PingOne to obtain data from your identity store.

Before you begin, you will want to consult with your identity provider management team to determine who should be able to authenticate to Venafi Platform via PingOne for Enterprise. You'll need that information near the end of the procedure below.

IMPORTANT While Venafi makes an effort to provide accurate information on third-party integration steps, these steps may differ for your service provider, especially as identity providers release new updates. If you have questions about how to use this third-party integration, we recommend you start with the vendor's documentation and support teams. These instructions should be considered a template, ***not definitive steps***. Your specific steps may vary, depending on how your organization integrates with each third-party platform.

To configure PingOne for Enterprise single sign-on

1. Log in to PingOne for Enterprise, and click **Applications**.
2. Navigate to **Add Application** > **New SAML Application**.
3. Give the application a descriptive name for your Venafi cluster, and provide a description and choose a category.
4. Click **Continue to Next Step**.
5. Next to SAML Metadata, click **Download**. We refer to this file as the *IDP Metadata XML file* in our documentation..

   Save this file to your Venafi Platform server in a place you can find it later.
6. Ensure the protocol version is **SAML v 2.0**.
7. Under Upload Metadata, click **Select File**, then browse to the Venafi Service Provider Metadata XML file you exported from Venafi Platform, and select it.
8. The following fields are described below:
   - The **Assertion Customer Service (ACS)** field will be automatically filled out from the uploaded Service Provider Metadata XML file.
   - The **Entity ID** will be automatically filled out from the uploaded Service Provider Metadata XML file. This is a unique string PingOne uses to identify the application when communicating with it.

- For **Application URL**, you can leave blank.

  This feature, if used, provides the starting URL for a user, if you don't want them being taken directly to the Aperture dashboard. For example, you could specify the SSH Protect dashboard, or the Certificate Inventory URL. This URL will be used when a user clicks on the Venafi application on their PingOne dashboard. This field is not honored if authentication was started by Venafi Platform. If you use this field, use the FQDN to the page.

- **Single Logout Endpoint, Response Endpoint, Binding Type**. These settings are not supported in this version of Venafi Platform, so leave blank.

- **Primary/Secondary Verification Certificate**. Since version 25.1 doesn't support signing authentication requests, leave blank.

- **Encrypt Assertion**. Since version 25.1 doesn't support encrypted SAML responses, leave blank.

9. Change the Signing option to **Sign Response**.
10. Leave the Signing Algorithm to the default, which is **RSA SHA256**.
11. If you want to force re-authentication for users, even if they already have an active PingOne session, select **Force Re-Authentication**.
12. If needed, modify the subject of the SAML assertion.

    By default, PingOne sends the username as the NameID within the subject of the SAML assertion. If you need to have something different sent instead (like email address), you need to define appropriate attribute mapping on this screen.

    More information can be found in PingOne's documentation.

13. In Group Access, click **Add** next to groups that should have access to Venafi Platform.

    If you want all users to have access, click **Add** next to **Users@directory**.

14. Review your settings, then click **Finish**.

> **IMPORTANT** When you test PingOne, if you get an error on a login attempt that says "SAML authentication failed" with an InvalidSignatureException, try disabling assertion signing in step 9, above. This is due to a problem in .NET.
>
> If disabling assertion signing doesn't work, please contact Venafi Support.

You are ready to finish configuring SSO in Venafi Configuration Console. See "Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML" on the next page.

Importing Identity Provider Metadata XML into Venafi Configuration Console for SAML

After you configure your identity provider (IDP), you are ready to go back into the Venafi Configuration Console to finalize the configuration. During this process, you will upload the IDP Metadata XML. This file contains configuration information that Venafi Platform needs to properly configure your SAML connection to the IDP.

This topic is part of Phase Three (of three) in Configuring SAML SSO authentication. For an overview of the complete process, see "Working with SAML for single sign-on (SSO)" on page 810.

To import IDP Metadata XML into Venafi Platform

1. Use Remote Desktop to connect to your Venafi server, and open Venafi Configuration Console.
2. Click the **Authentication** node.
3. Click the **SAML** component.
4. In the **Actions** panel, click **Properties**.
5. [Conditional] If requested, enter a master administrator username and password for Venafi Platform.
6. [Conditional] If not previously selected, choose your **IdP Vendor** from the drop-down list.
7. In the **Export and import SAML metadata** section, click **Import identity provider file**
8. Browse to the location of the IdP SAML file on your system, click the file, then click **Open**.
9. If your IDP support it, you can provide a **Logout URL**.

   If a value is not provided, you won't see a Logout link in the menu. Of the IDPs tested by Venafi, only Azure supports logging out by URL.

   If there is no Logout link, users will close their browser to terminate a session.
10. Click **Save**.

    The **SAML Properties** window closes.
11. In the **Actions** panel, click **Enable**.

Managing the SAML certificate in TLS Protect

The IdP Metadata XML file contains a TLS certificate that is automatically enrolled in TLS Protect at the *monitoring* level. This means you can see the SAML certificate in the policy tree, and you can see (and monitor) its expiration like you do for your other certificates.

The enrollment level is monitoring because TLS Protect can't renew and provision a new certificate. To renew this certificate, you must export a new IdP Metadata XML file from your identity provider and upload it into the Venafi Configuration Console. When you import a replacement IdP Metadata XML file, the old certificate is placed in the history of the new certificate.

The location of the certificate in the policy tree is shown in the **SAML Properties** panel after you upload your IdP Metadata XML.

What's Next

If everything is configured correctly, SAML authentication should now work. We recommend opening another browser or incognito window and open Aperture. You should be redirected to your IDP login page. If you enter valid credentials, you should be taken to Aperture.

If you are having troubles, check out some "SAML troubleshooting tips" below.

SAML troubleshooting tips

If your SAML SSO integration is not working, here are some things you can try.

Check the Venafi Platform logs. Venafi Platform has very detailed logging for SAML Authentication when an error is encountered. Start with the Venafi Configuration Console Log Viewer. For example:

1. In Venafi Configuration Console, Expand the **Venafi Event Viewer** node.
2. Right-click on **Custom Views** and click **Create Custom View**.
3. In the **Logged** field, choose **Last Hour**.
4. For **Event Sources**, choose the parent **SAML Group** node, then click **OK**.
5. Give the custom view a **Name**, like `SAML Last Hour` and place it in the **Custom Views** container.

You now have an easy to use log view for troubleshooting SAML issues.

Enable Debug Logging for your UI Server. In Policy Tree on the Platform tree, you can select your servers that have "Web Console" enabled and activate debug logging temporarily. Additional logs will be stored, like your SAML Assertion, which is helpful for understanding what was sent and received between Venafi Platform and the SAML Identity Provider (IDP).

Make sure your FQDNs are configured. By default, email notifications and your SAML configuration use your windows machine `hostname` to build URLs. This is typically *not* the URLs you want to use in either lab or production environments. Instead, we recommend putting in a fully qualified domain name (FQDN)

that matches the trusted Venafi Operational Certificate you have installed on Venafi Platform. Once this is set, you may need to re-export your Service Provider Metadata XML file from the Authentication node of the Venafi Configuration Console, and use the updated file to re-configure your settings with the Identity Provider.

Type the correct domain name in your browser. If your Venafi Platform is configured to use `platform.example.com` don't use the machine's IP address or `localhost` when accessing your SAML-enabled server. An error can occur, because Venafi Platform will redirect you to your identity provider. Your IDP will generate a signed SAML response using the domain name you configured (for example, `platform.venafi.com`) If the domain name that your IDP uses is not the same as the one you entered in your browser, Venafi Platform will reject the SAML response from your IDP for security reasons.

Check the value in the `NameID` within the subject section of the SAML assertion of your SAML Response. A SAML Response can be several hundred lines long, but in every response you should see a basic structure to include a `NameID` that tells your server "this is the user who I am authenticating."

```
<samlp:Response>
    <saml:Assertion>
        <saml:Subject>
            <saml:NameID>aaron.hixson@venqa.venafi.com</saml:NameID>
        </saml:Subject>
    </saml:Assertion>
</samlp:Response>
```

You should know what type of identification you are using to identifying users. We recommend using a `User Principle Name` (UPN) because it always uniquely identifies a user within a given directory. However, there are other alternatives.

When looking at the SAML response, you're looking for two things:

1. Check that the SAML Response `NameID` matches the user identifier you are expecting. If yes, go to the next step.
2. Turn off SAML on Venafi Platform and authenticate to Aperture as a user from that Identity Provider. For example, if your IDP uses Active Directory, try logging in to Aperture with a valid AD user and password. Once in Aperture, take the string from the `NameID` and try to search from the user. In our example, search for a `UPN` of `aaron.hixson@venqa.venafi.com`. If there are no results, then you probably have one of the following problems:
    - Your User Search Expression for your Identity Provider doesn't include the attribute for user class objects that this attribute is stored on.

For example, for UPN you didn't change your Active Directory user search expression to: `(&(|(ANR=$search$)(userPrincipalName=$search$))(objectCategory=$userclass$))`

- If using Active Directory, you may have expected the attribute to be included in your directory's "Ambiguous Name Resolution" (ANR). By default, Venafi Platform's Active Directory driver searches for users using ANR. While Microsoft documents what the default attributes are for ANR, your Active Directory Administration team may have removed or added attributes that are different from Microsoft's default settings.
- Your identity directory does not have the values you think it does. Let's say for example your Identity Provider has `employee ID`, and you thought Active Directory or LDAP also had an `employee ID`, if that is not the case, you should switch to a different unique attribute like Universal Principal Name (UPN). As mentioned before, a good test is to log into Aperture and try to search for the user using the desired attribute, if nothing shows up, then that problem needs to be resolved first.

Ensure you are using a unique identifier. If you are trying to use something like `email`, `username`, or `SAMAccountName` as the value in your `NameID`, it's possible that these values are returning multiple results when Venafi Platform searches your IDP's directory. When an Identity search returns multiple entries, the SAML Assertion is rejected because the lookup for a user is ambiguous. A match will only be made if there is one–and only one–user that matches the `NameID` of the SAML Assertion subject.

When looking at the log, if you see a log event similar to the following, this is likely your problem.

> Ambiguous identity lookup by name id (admin). Found identity entries: (local:{c6b377a2-8e8a-4cd8-cee9-9690f0d988a3}, LDAP+odsee:6c512d81-48f711a2-80d19f9-b115de56).

Your IDP is not signing the SAML Response. Venafi Platform requires SAML Responses to be signed, but with the exception of Okta, all of the IDPs that Venafi supports, by default, only sign the *assertion* within the response. When setting up your IDP to work with Venafi Platform, make sure Venafi Platform's application profile is configured to sign the *response*.

Time Sync Problem. Venafi Platform requires that the SAML Assertion include the `NotOnOrAfter` parameter within the `SubjectConfirmationData` of the assertion. This is to prevent the possibility of misuse of the signed XML document. Venafi Platform allows for a clock skew of 180 seconds (3 minutes). Check to make sure that the system time of your IDP and the system time of your Venafi servers are all accurate.

Other tips and information

- We suggest you try the Firefox SAML Tracer Extension, a valuable tool that picks through the network traffic and highlights the SAML XML documents that Venafi Platform and your SAML IDP are sending back and forth through your browser. While you can get this information if Venafi Platform is in Debug Mode, and you look through the logs, this extension provides real-time information, which is faster and simpler than using the system logs. In addition, in some customer environments, Debug Mode isn't allowed or is not a practical solution.

  > **TIP** Make sure you have the extension open *before* you visit your IDP or Venafi Platform's web console. The SAML Tracer Extension only captures traffic when the extension window is open.

- If you're looking for the Logout button in Venafi Platform's navigation, you should know that the Logout button isn't visible when SAML single sign-on is enabled. In Venafi Platform 25.1, we don't support SAML Single Log Out (SLO). What we do support is a **Logout URL**. If your IDP supports ending the session by simply visiting a URL, you can place that URL in the **Logout URL** field. After you set this, restart IIS and you should see the Logout link in the User menu of the Venafi Platform web console.

  As far as we know, Azure may be the only supported IDP that permits logging out by just visiting a URL. Azure users can use the following **Logout URL**:

  ```
  https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
  ```

14

Setting up Certificate Verification for securing outbound HTTPS connections

The Certificate Verification settings allow a secure HTTPS connection for a server that presents a valid certificate, which is not currently on a Certificate Revocation List (CRL). There are two parts to the setup:

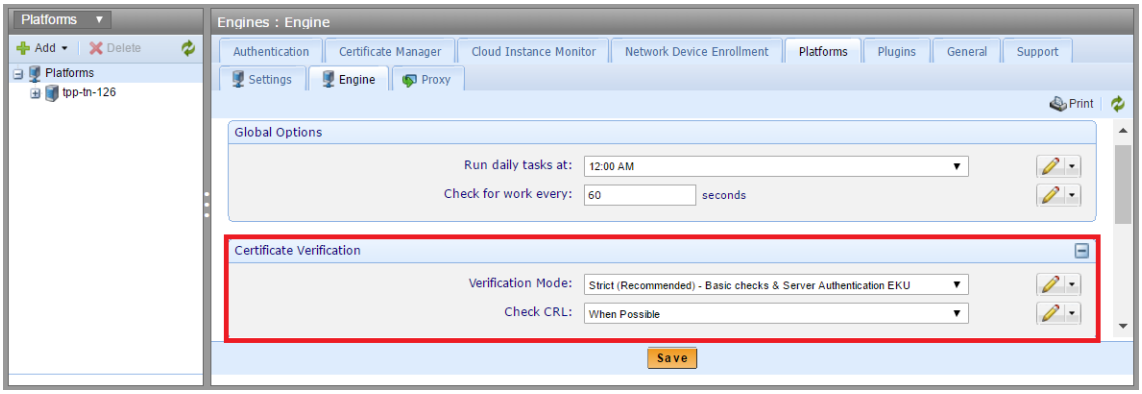
- You can use the **Verification Mode** to confirm that the certificate is valid. Based on the setting, Trust Protection Platform checks various fields on the certificate. If the information is valid, Trust Protection Platform allows a secure connection with the server.
- You can use the **Check CRL** setting to determine the status of the certificate that the server presents at the time of connection. If the certificate appears on a (CRL), Trust Protection Platform will refuse the connection even if the certificate is valid.

> **NOTE** Don't confuse this setting with CRL Verification, which periodically checks stored Trust Protection Platform certificates. For more information, see Enabling CRL Verification.

To set up certificate verification

1. From the TLS Protect menu bar, click Policy Tree, then open the **Platforms** tree.
2. Click the root of the **Platforms** tree to see the individual Trust Protection Platform servers.
3. Do one of the following:

- To make global changes, click the **Engine** tab.
- To configure a specific server, select a Trust Protection Platform server, and then click **Settings**.



4. Scroll down to the **Certificate Verification** section.
5. In the **Verification Mode**, select one of the following options and set the level of certificate checking:
   - **None (Not Recommended) - No verification**: (Default) Allow the connection to the server. If the certificate would have failed the Basic or Strict certificate verification, log a Certificate Verification Warning event message.
   - **Basic - Checks expiration, revocation, common name mismatch & root chain**: Check for an expired certificate, CN mismatch, invalid chain, inability to chain back to a trusted root, and whether one or more of the certificates in the chain has an invalid CA certificate. If any of these checks are invalid, refuse the connection and log a Certificate Verification Failed event message. If the certificate would have failed the Strict certificate verification, log a Certificate Verification Warning event message.
   - **Strict (Recommended)- Basic checks & Server Authentication EKU**: Do the same checking as with the Basic certificate verification. Reject a certificate if it failed the Basic certificate verification. Also, if the Server Authentication (EKU) is present on the certificate, verify the value. Reject an otherwise valid server certificate that lacks the Server Authentication Purpose information in the EKU. For rejected certificates, refuse the connection with the server and log a Certificate Verification Failed event message.
6. In the **Check CRL**, select one of the following options:

- **Never**: Bypass CRL checking. Establish the HTTPS connection based on certificate values.
- **When Possible**: (Default) If the certificate is valid, determine whether it is currently on the CRL. If the certificate is revoked, refuse the connection and log a Certificate Verification Error event message. However, if the CRL cannot be retrieved, allow the connection.
- **Always**: If the certificate is valid, always determine whether it is currently on the CRL. If the certificate is revoked or cannot be verified on the CRL, refuse the connection. Log a Certificate Verification Failed event message.

7. If you selected *None (Not Recommended)* for Verification Mode, you need to specify whether the system should **Log warnings when problems are detected with certificate**.
   - *Yes*: Warning events are logged.

     Note that if the Trust Protection Platform server does not trust the chain, or if there is a self-signed certificate, you may see *many* certificate verification warning events logged.
   - *No*: (default): Warning events are not logged.
8. Click **Save**.
9. Restart IIS and all Venafi services.

IMPORTANT Syslog channel drivers can't recognize changes you make to either the **Allowed Outbound SSL/TLS Versions** settings or **Certificate Versions** settings. Therefore, following any changes to those settings, please restart the Venafi Log Server Windows service. For details, see "Manually stopping and starting the log server service" on page 432 in the *Log Server Administration Guide*.

15

Trust Protection Platform components

The following is a list of components that are available for selection in Venafi Configuration Console. Any component that is not selected during installation can be enabled later in the configuration console.

Some components can't be added to your system. For example, if IIS is not installed, or if you don't have a valid license for a specific product, related components won't be available.

Component	Answer file key	Products	Description
ACME Service	Acme	TLS Protect, Client Protect	Provides certificate automation via an Automated Certificate Management Environment (ACME). An HTTPS server is set up and configured to automatically obtain a browser-trusted certificate without any human intervention. A certificate management agent runs on the web server. **IMPORTANT** Venafi's implementation of the ACME protocol was designed and tested for use with the following clients: *certbot*, *win-acme*, and *acme.sh*. If you're using a different client, you might encounter limitations. For example, your alternate ACME client might use portions of the ACME protocol that aren't supported by Venafi's integration with the certbot and win-acme clients.
Authentication Server	AuthServer	Platform	Provides authentication for REST access for web components.
Automatic Layout Manager	AutoLayout	Platform	Enables Placement Job feature, allowing you to reconcile duplicates and organize certificates and devices in folders based on placement rules. If this feature is installed during installation of Venafi Trust Protection Platform, it can be enabled or disabled either in the Venafi Configuration Console, or in Policy Tree on the Platforms tree.

Component	Answer file key	Products	Description
			If you have multiple servers in your cluster, you may want to enable this feature on some, but not all, of the servers in the cluster for performance reasons. That would enable one server to be running the placement jobs feature without impacting the performance of other servers in the cluster.
Bulk Provisioning Manager	BulkProvisioning	TLS Protect	Provisions keys and certificates to one or more devices simultaneously.
CA Import	CAImport	TLS Protect, Client Protect	Automatically imports certificates from supported Certificate Authorities.
Certificate Lifecycle and Monitoring	Certificates	TLS Protect, Client Protect, CodeSign Protect	Provides certificate lifecycle management. Responsible for certificate-related tasks such as expiration notifications, issuance, renewal and revocation, and for provisioning of certificates to devices.
Certificate Revocation Monitoring	Revocation	TLS Protect, Client Protect	Provides the ability for Trust Protection Platform to provide CRL Distribution Point monitoring. Monitors the revocation status of all certificates in inventory at least daily. Allows you to do an on-demand revocation check for an individual certificate in either Aperture or Policy Tree. Monitors OCSP and CDP endpoint validity. This component does not control your ability to revoke certificates; this component adds the ability to monitor for revocations and to monitor CDP and OCSP endpoints.

Component	Answer file key	Products	Description
			IMPORTANT Certificate Revocation and CDP Monitoring is a feature that must be enabled when you install Trust Protection Platform in the Venafi Configuration Console. This module is *disabled* by default if you are upgrading from a version of Trust Protection Platform prior to 19.2. You will need to enable it manually on at least one engine if you want to do revocation checking and CDP monitoring. When you enable this module on multiple engines, all must have equal access to all CDP and OCSP endpoints. If a particular engine does not have the same network access as other engines, then the service module should be disabled on that engine with restricted access. If you see sporadic network access or "unable to connect" statuses for your CDP or OCSP endpoints (either in the Roots tree, or in the logs), it is likely that one of your engines does not have access to reach those endpoints. CDP Monitoring and Revocation Checking does *not* honor engine partitioning in the Policy tree.
Client REST	Client	Platform	Enables communication between agents and Trust Protection Platform.

Component	Answer file key	Products	Description
Code Signing Client Distribution	ClientDistribution	CodeSign Protect	Enables a web page that provides helpful scripting information and links for downloading CodeSign Protect clients. You can access the page by adding `/csc` to your Trust Protection Platform URL, such as: `https://TPP-Server-Name/csc` For more information, see Using the CodeSign Protect Client Downloads page.
Code Signing Key Server	KeyServer	CodeSign Protect	Provides functionality to set up a JWK key server and a GPG key server to store public keys and make them publicly available through a RESTful HTTP request. For more information, see GPG public key server.
Enrollment over Secure Transport Service	EstService	TLS Protect, Client Protect	This service provides certificate enrollment capability for devices via the Enrollment over Secure Transport (EST) protocol. For more information on EST, see Certificate enrollment via EST protocol.
HSM Backend	HsmBackend	CodeSign Protect	Provides virtual HSM capability within Trust Protection Platform for code signing. This allows Venafi CodeSign Protect clients to request signing operations using private code signing keys that are managed by Trust Protection Platform.

Component	Answer file key	Products	Description
Key Lifecycle and Monitoring	KeyManager	CodeSign Protect	Provides key lifecycle management. Responsible for tasks such creating new keys and monitoring key expiration. This component is required for GPG and .NET CodeSign Protect Environments, as well as for SSH Protect.
Kubernetes Discovery Manager	JSSDiscovery	TLS Protect	Provides a way to monitor TLS certificates used on clusters managed by Venafi TLS Protect for Kubernetes. With the Kubernetes discovery feature, administrators can create new discovery jobs which import certificates from all Kubernetes clusters registered to Venafi TLS Protect for Kubernetes.
Network Device Enrollment	Scep	TLS Protect, Client Protect	Enables devices to use the SCEP protocol to request certificates from Trust Protection Platform. You would want to enable this feature if you have SCEP-enabled devices or applications and you want those devices and applications to be able to get certificates directly from Trust Protection Platform. This feature is frequently used with mobile-device management solutions. For more information on configuring Network Device Enrollment, see Managing network device enrollment (NDE) of the *Venafi Trust Protection Platform Certificate Management Guide*.

Component	Answer file key	Products	Description
Network Discovery	Discovery	Platform	Runs the Network Discovery surveys configured in your system's Discovery objects. During a Network Discovery, the Discovery server scans designated IPv4 address ranges and ports to identify SSL certificates. For more information on discovering network certificates, see Discovering certificates and keys in the Venafi Administration Guide.
Object Monitoring	Monitoring	Platform	Monitors SSH key and credential objects for expiration and generates expiration notifications. For more information on logging and event notifications, see Notification and logging overview in the *Venafi Trust Protection Platform Administration Guide*.
Onboard Discovery Manager	OBDDiscovery	TLS Protect	Configuring onboard discovery jobs lets you automate the process of provisioning by adding devices to one or more specific policies. You then have control over the placement of discovered certificates without having to manually update jobs or reorganize certificates after they've been discovered.
Reporting	Reporting	Platform	Generates and distributes pre-defined and custom reports.
SSH Certificate Lifecycle and Monitoring	SSHCertificates	SSH Protect	Allow you to use SSH Protect to manage SSH Certificates.
SSH Key Detection and Remediation	SSH	SSH Protect	Secures and protect SSH keys and systems through discovery, reporting, policy enforcement, and remediation.

Component	Answer file key	Products	Description
Time Stamp Service	TimeStampService	CodeSign Protect	Provides an RFC 3161-compliant time stamping service for code signing. This service allows you to use either your own time stamping certificate or to specify a list of time stamping proxies. Once configured, you can then specify Trust Protection Platform as your time stamping server.
Validation	Validation	TLS Protect, Client Protect	Runs the network and onboard validation processes. Network validation verifies a certificate or key is installed on the target system, then determines if the correct certificate is being used. For more information on validating certificates and applications, see SSL/TLS network validation of the *Venafi Trust Protection Platform Certificate Management Guide*.

Component	Answer file key	Products	Description
Web Console	WebConsole	Platform	Web-based management interface. Installs both Policy Tree and Aperture. At least two Venafi servers needs to have Web Console enabled. If Web Console is configured on two different servers, you can disable this component. Server requirements for Web Console are outlined in System requirements for Venafi components.
Web SDK	WebSDK	Platform	Extend your custom environments by integrating them with Venafi solutions using the Venafi Web SDK code library. For more information, see About this guide in the *Trust Protection Platform Developer's Guide*.

Configuring the Validation Manager module

The Validation Manager module runs Network validations of SSH Server Key, Certificate, and Application objects. It also performs Onboard Validations of Application objects. For more information on system validation, see Validation Overview in the *Venafi Trust Protection Platform Certificate Management Guide*.

To configure the Validation Manager module

1. From the TLS Protect menu bar, click Policy Tree.

   IMPORTANT You must have the View and Write permissions to the Validation Manager module.

2. Click the arrow then select the Platforms tree from the list.
3. In the Platforms tree, select the Validation Manager module.
4. Configure the Validation Manager object settings, and then click **Apply**.

Validation Manager Module Configuration Settings

Option	Description
Validation Module Tab	
Settings	
Disabled	Disables the Validation Manager module. No validation scans occur when the Validation Manager module is disabled.
General Tab	
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Configuring the Reporting module

The Reporting module generates the Venafi Trust Protection Platform reports as per their designated schedules. For more information on reports, see "Managing system reports" on page 977.

To configure a Reporting module

1. From the TLS Protect menu bar, click Policy Tree.

   IMPORTANT You must have the **View** and **Write** permissions to the Reporting module in order to configure it.

2. In the tree drop-down menu, select **Platforms**.

The expanded platforms tree shows a list of all the servers that connect to the database.

3. In the platforms tree, expand a server, then click the **Reporting** module.
4. Configure the Reporting object settings, and then click **Apply**.
5. Repeat for additional servers that send reports, as necessary.

Field	Description
Reporter Module	
Settings	
Disabled	Disables the Reporting module. Reports cannot be generated nor can Trust Protection Platform populate the Licensing tab in the Dashboard when the Reporting module is disabled.
SMTP Options	The SMTP settings provide the information Trust Protection Platform requires to mail reports to the recipients designated in the report configuration. For more information, see "Managing system reports" on page 977. The following options are required to enable the Reporting module.
Host	Hostname or IP address of the SMTP server. You can append the port number to the host. For example: 192.168.3.45:25. If a hostname is specified, only the first resolved address associated with that name is used.
Credentials	Username credential required to authenticate with the SMTP server. Configure this option only if SMTP authentication is configured on your SMTP server. Otherwise, all notifications routed through this Channel object will fail.
Sender	Name that appears in the From: line for all messages sent from the Reporting module. Some SMTP servers require this field to be a valid email address. If this is required by your SMTP server, make sure you provide a valid email address, such as username@yourcompany.com.

Field	Description
Use TLS	Configures the Reporting module to use Transport Layer Security (TLS) to email reports. Select this option only if your SMTP server is configured to support TLS. Otherwise, all notifications routed through the Reporting module will fail.
Log Delivery	Configures the Reporting module to log an event every time it emails a report. If it successfully emails the report, the driver logs an Report Sent event. If the notification fails, the driver logs an Report Delivery Error event. To help you troubleshoot the message failure, SMTP Message Failure events provide the exception details returned from the SMTP server.
General Tab	
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Configuring the Monitor module

The Monitor Manager module generates certificate and SSH key expiration events. For more information on managing the parameters under which the Monitor Module generates expiration events, see "Configuring expiration event intervals" on page 507.

To configure the Monitor module

1. From the Platform menu bar, click **Policy Tree**.

   NOTE You must have the View and Write permissions to the Monitor module.

2. Select the **Platforms** tree from the Tree drop-down menu.

3. In the Platforms tree, select the **Monitor** module.
4. Configure the Monitor object settings, and then click **Apply**.

Validation Manager Module Configuration Settings

Option	Description
Monitor	
Settings	
Disabled	Disables the Monitor module. At least one Monitor module must be enabled in your encryption system. If all Monitor modules are disabled, no certificate or SSH key expiration events are generated . If multiple Monitor modules are enabled on Trust Protection Platform servers throughout your network, the modules coordinate expiration event monitoring so expiration events are not duplicated.
General Tab	
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Configuring the Discovery module

The Discovery module scans the IPv4 address and port ranges configured in your system's Network Discovery objects. For more information about discovery, see Discovering certificates and keys.

IMPORTANT You must have the *View* and *Write* permissions to the Discovery module.

To configure a Discovery module

1. From the Platform menu bar, click Policy Tree.
2. Select the **Platforms** tree from the Tree drop-down menu.
3. In the **Platforms** tree, select the **Discovery module**.
4. Configure the Discovery module object settings, and then click **Apply**.

The following table describes available settings and options for the Discovery module.

Field	Description
Discovery module	
Settings	
Disabled	Disables the Discovery module. No discovery scans occur when the Discovery module is disabled.
Connection Timeout	Amount of time (in seconds) that Discovery waits for connection results before making another attempt. ■ Default = 10 ■ Minimum = 1 ■ Maximum = 300
SSL/TLS Handshake Timeout	Amount of time (in seconds) that Discovery waits for a successful SSL/TLS handshake before making another attempt. ■ Default = 10 ■ Minimum = 1 ■ Maximum = 300

Field	Description
Pause between connection attempts	Amount of time (in milliseconds) that Discovery waits between connection and handshake attempts. ■ Default = 1
Socket Load	Percentage of available Windows sockets used by the Discovery engine. ■ Default = 90% ■ Minimum = 5% ■ Maximum = 90% Discovery has the potential to run slower if you don't give it more resources. To optimize Discovery performance, you can modify the Registry to increase the maximum number of ephemeral ports. For more information, see the following Microsoft Support Document: http://support.microsoft.com/kb/196271.
Processing Window	The Discovery module processes discoveries only during the designated processing times. This means that if you click **Run Now** to manually run a discovery, the discovery is placed in the discovery queue, but does not run until the designated processing times.
Run Between	Select the time span during which you want this Discovery module to process discoveries.

Field	Description
Run only on	Select the specific days of the week you want this Discovery module to process discoveries.
General Tab	
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). . If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

16

Using policies to manage encryption assets

Policies provide a hierarchical framework for managing configuration and objects within your environment, much like hierarchical directories such as Active Directory.

Policies can contain system objects (such as Devices, Applications, and Certificates) as well as other policies. Each policy enables you to set the configuration for each object type contained below it. For example, if several IIS Application objects are contained within a policy, one or more of the configuration attributes for those IIS objects can be defined on the policy. Consequently, policies can be used to standardize object configuration parameters and enforce security requirements throughout your encryption environment.

This section provides the information you need to manage your encryption resources using policies:

This chapter contains the following topics:

How policies work 860

How policies work at the object level 860

How policies work at the value level 861

Locking policy values 863

Policy structure examples 865

Managing your policies (folders) 874

How policies work

Policies allow administrators to define global configuration parameters for encryption resources associated with that policy. For example, within a policy, you can define certificate settings that you want to standardize in your organization such as the certificate Contact, Subject DN, management type (Monitoring, Enrollment, Provisioning, or Unassigned), CA Template, and key strength.

In the Trust Protection Platform Administration Console, policies can contain one or more system objects, including Devices, Certificates, Application Workflows, CA Templates, Applications or even other policies.

> **NOTE** Application objects cannot be created directly under policies; they can be created only under Devices.

When a system object is defined in a policy in the Trust Protection Platform Administration Console, the object and its corresponding resource are associated with the policy and are subject to the policy's settings. For example, if you configured certificate settings on a policy, Trust Protection Platform would read those values for the policy's subordinate certificates. Thus, policies can be used to standardize object configuration parameters and enforce security requirements.

To understand how this works, it is helpful to first discuss how Trust Protection Platform applies policies to resources in your encryption environment, then discuss how individual policy values are implemented. The following sections review how policy settings are defined within a policy, and then how those policy settings apply in your encryption environment.

How policies work at the object level

Policy values are read every time Trust Protection Platform accesses an object in the folder tree—this includes when the object is viewed in the Trust Protection Platform console as well as when Trust Protection Platform processes the object (for example, a certificate renewal). To determine an object's configuration, Trust Protection Platform starts with the root policy at the top of the tree, then reads down through the policy hierarchy until it arrives at the object. Trust Protection Platform applies the value of object attributes based on the following priority:

1. Locked policy values
2. Values defined at the object level
3. Unlocked policy values

This means that the current policy values are always applied, in real time, to objects in the tree. If you update a policy or move an object under a different policy, Trust Protection Platform always applies the current policy values. Current policy values are also applied when you create new objects in the tree.

It is important to remember, however, that while Trust Protection Platform always applies current policy values to objects in the tree, it does *not* apply policy values—or any object configuration, for that matter—to existing resources in your encryption environment until a certificate or key is deployed or renewed. For example, a policy definition for the Apache Web server's Certificate and Private Key files is not written to the Apache Web server itself until the certificate and private key are pushed to that server or the certificate is renewed. Trust Protection Platform can tell you that an existing certificate is out of policy, but it cannot revise the certificate and bring it into compliance with current policy unless the certificate is renewed or replaced.

> **NOTE** To determine if a certificate complies with current policy, go to the Compliance tab in the Certificate object configuration. For more information, see Determining Certificate Compliance in the *Venafi Trust Protection Platform Certificate Management Guide*.

This is the connecting point between the virtual configuration of the Policy tree and the actual configuration of your encryption system resources. Policies allow you to define the parameters under which certificates are created and deployed in your encryption environment.

How policies work at the value level

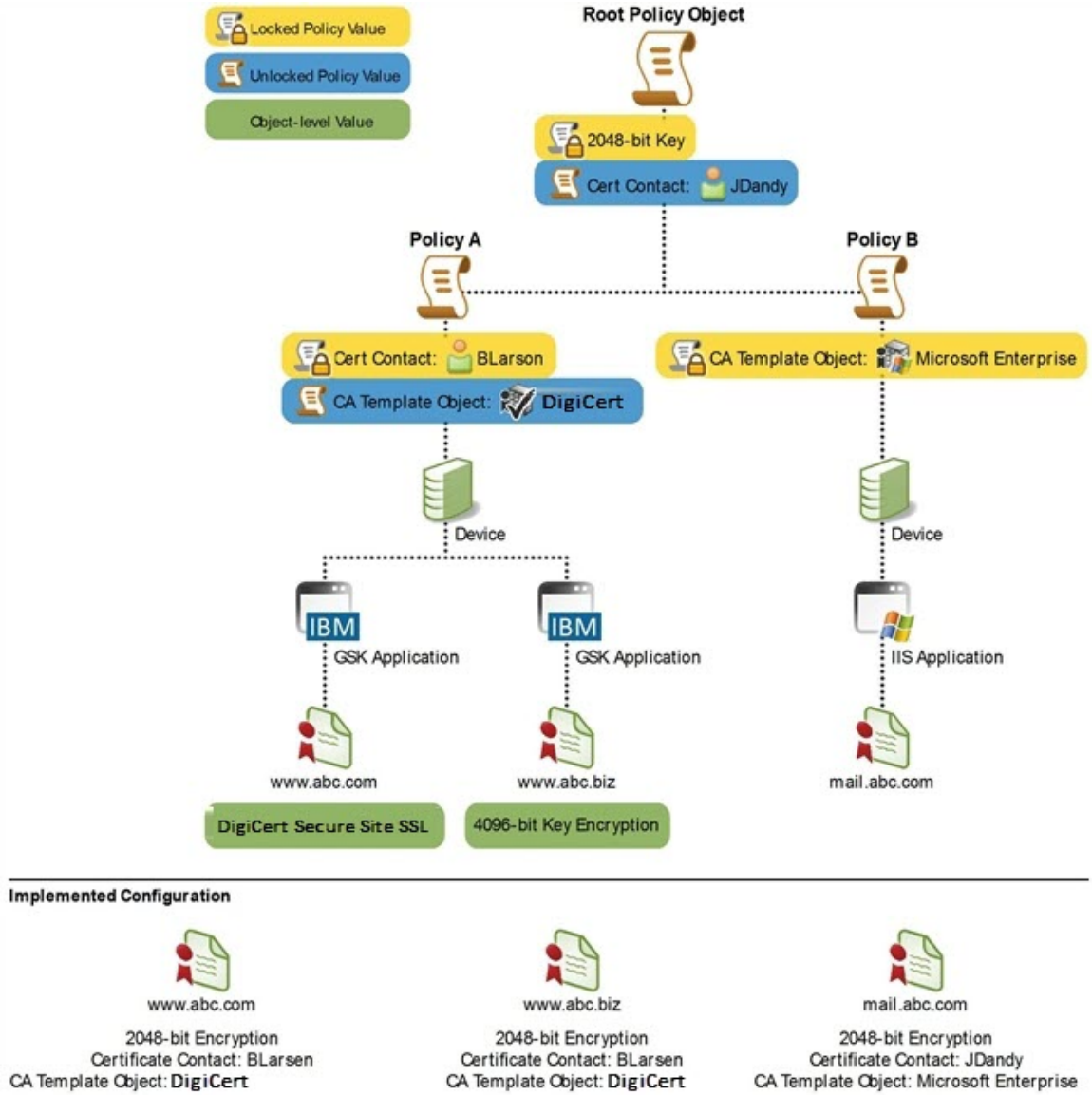
How an individual policy value is implemented depends on whether the value is locked or not. When Trust Protection Platform looks up an object's configuration in the tree and it encounters a locked policy value, it stops reading down the tree. A locked value is the only value read for all subordinate objects in the tree. It doesn't matter what is actually configured in the subordinate objects; Trust Protection Platform reads only the first locked policy value in the tree.

For information on locking policy values, see "Locking policy values" on page 863.

If you do not lock a policy attribute, the attribute functions as a default value—that is, it appears as the default option when you create new subordinate objects—but it can be overwritten at the object level. Unlocked policy values flow down the tree, with the lowest value taking precedence. That means that when

Trust Protection Platform looks up an object's configuration in the tree and it encounters an unlocked policy value, it continues reading down the tree until it reaches the object configuration. Attributes defined at the object level always take precedence over unlocked values inherited from policies higher up the tree.

To illustrate this point, let's consider the following configuration:



The Root folder, folder A, and folder B each define settings for Certificate objects. Two Certificate objects–www.abc.com and www.abc.biz–have their own settings as well.

With the object configurations specified in the example, the configuration that Trust Protection Platform actually implements for the three certificate objects is as follows:

Certificate	Key Strength	Certificate Contact	CA Template Object
www.abc.com	2048-bit	Certificate Contact: BLarsen	DigiCert CA Template Object
www.abc.biz	2048-bit	Certificate Contact: BLarsen	DigiCert CA Template Object
mail.abc.com	2048-bit	Certificate Contact: JDandy	Microsoft Enterprise CA Template Object

Locking policy values

When you define an attribute within a policy, you can lock or unlock the value. Locked attributes cannot be modified in objects contained by that policy, including sub-policies. Unlocked attributes function as suggested values; they can be accepted or overwritten in the subordinate object configuration.

By default, policy values are unlocked.

For more information, see "Locking and unlocking policy values" below.

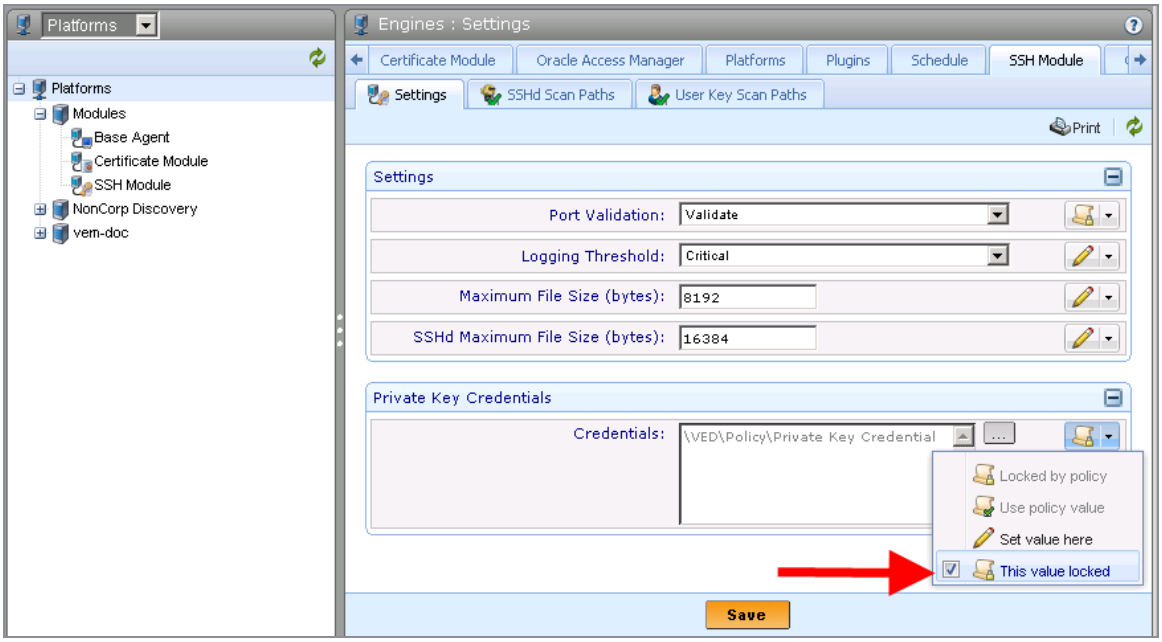
Locking and unlocking policy values

The Root Platform and Module objects are policies. They are used to define and enforce policy settings for subordinate objects in the Platforms tree. Configuration settings defined in the Root Platform and Module objects are inherited by the subordinate Agent Module objects. However, how those settings are implemented depends on how they are defined in the parent object. When you define an attribute within a parent object, you can lock or unlock the value.

Locked attributes cannot be modified in subordinate objects. Unlocked attributes, on the other hand, function as suggested values; they can be accepted or overwritten in the subordinate Agent modules.

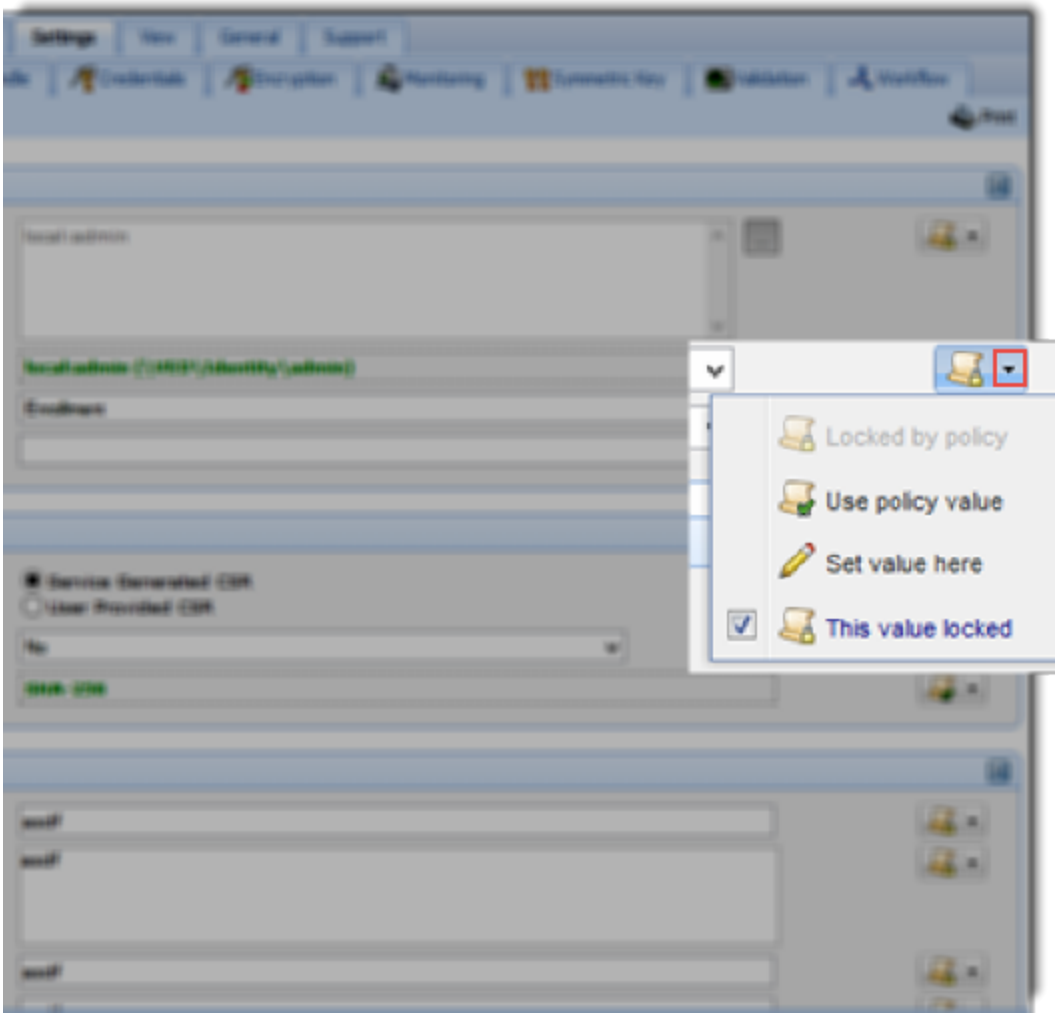
By default, policy values are unlocked.

The following graphic shows the policy configuration for the Root Platform object. The Port Validation and Private Key Credential values for the SSH Module are locked while the Logging Threshold and Maximum File Size values are unlocked.



To lock a policy value in Policy Tree

- Click the arrow to see a list of choices for setting or locking that value.



Policy structure examples

The efficiency and effectiveness with which Trust Protection Platform manages your encryption system resources depends on how you deploy your system policies. The following sections provide a brief overview of different ways you can deploy policies in Trust Protection Platform. When you create your own policy structure, you can adapt these strategies to meet your own needs and requirements. The objective is to create a policy structure that enforces your organization's security requirements, supports your native framework of system administration, and keeps your encryption system resources at an optimal configuration.

Management level

Some organizations support certificate Monitoring, Enrollment, Provisioning, and Unassigned in the same policy tree. For example, you may fully provision internal certificates such as your mail server and intranet certificates. External certificates, such as those used on your corporate Web site, may be more strictly controlled and, therefore, managed at the Enrollment level. Third-party certificates that are critical to your business, such as vendor or partner certificates, may be managed at a Monitoring level so you can track the certificate life cycles.

To effectively manage these types of environments, you may create separate policies for each management level.

One significant advantage of this policy structure is that it allows you to separately manage the certificate configuration requirements for each management level. In this example:

- The Provisioning policy requires 2048-bit certificates and applies a Workflow object that restarts the Apache Web server after it installs the new mail server certificate and private key.
- The Enrollment policy's certificate configuration requires user-provided CSRs and applies a Workflow object that requires a certificate approval for the CSR enrollment.
- The Monitoring policy generates certificate expiration events several months before the certificate expires so you have adequate time to work with your partners and vendors to ensure the certificates are renewed and functional.
- **Unassigned**: Unlicensed Trust Protection Platform certificates and keys that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.

This policy structure also allows you to group the encryption assets related to each management level. In this example:

- The Provisioning policy contains the Device and Application objects that consume provisioned certificates, the CA Template object used to renew provisioned certificates, and the Workflow object that restarts the Apache Web server.
- The Enrollment policy contains the CA Template object used to renew the external certificates and the Workflow object that requires a certificate approval for the CSR enrollment.
- The Monitoring folder contains only the monitored third-party certificates.
- **Unassigned**: Unlicensed Trust Protection Platform certificates and keys that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.

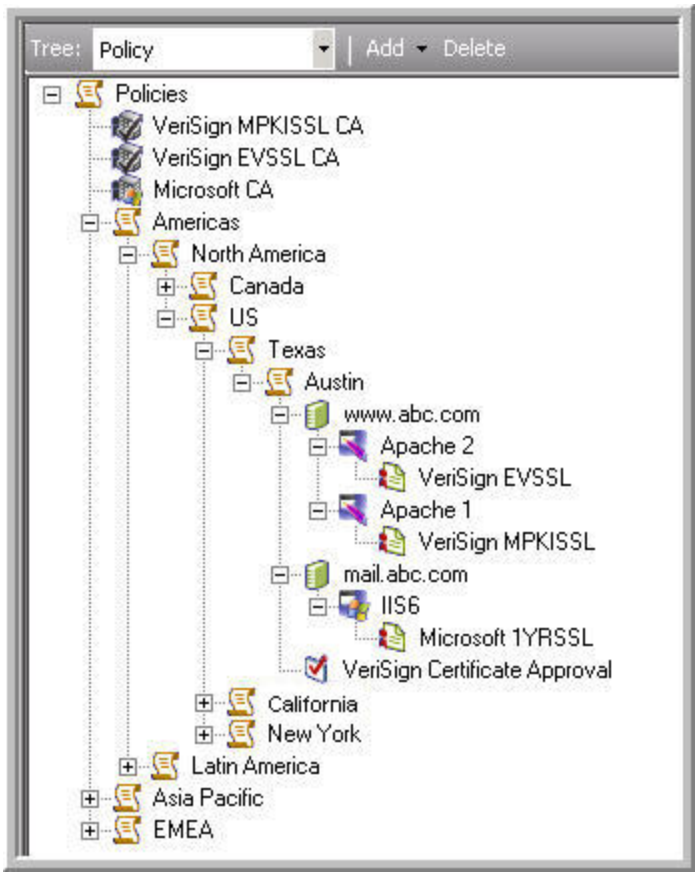
Finally, this policy structure provides a natural framework to distribute your system administration. In this example:

- The administrators responsible for the mail and intranet servers are the contacts for the objects under the Provisioning policy.
- The Symantec administrator is the contact for the objects under the Enrollment policy because this administrator submits the CSRs to Symantec for renewal.
- The person responsible for vendor and partner relations is the contact for the objects under the Monitoring policy because this person works with these parties to ensure the third-party certificates are renewed and functional.

Organizational Folder Structure

The following example represents a multinational organization; however, the same structure can be created using business units, divisions, departments, functional groups, and so forth.

Figure 16.1: Organizational Folder Structure



An organizational folder structure allows you to group encryption assets by location or other organizational boundary. In this example, we see the encryption system assets located in Austin, Texas. Resources that are shared between locations, such as the Symantec and Microsoft CA Template objects, are located under the root folder.

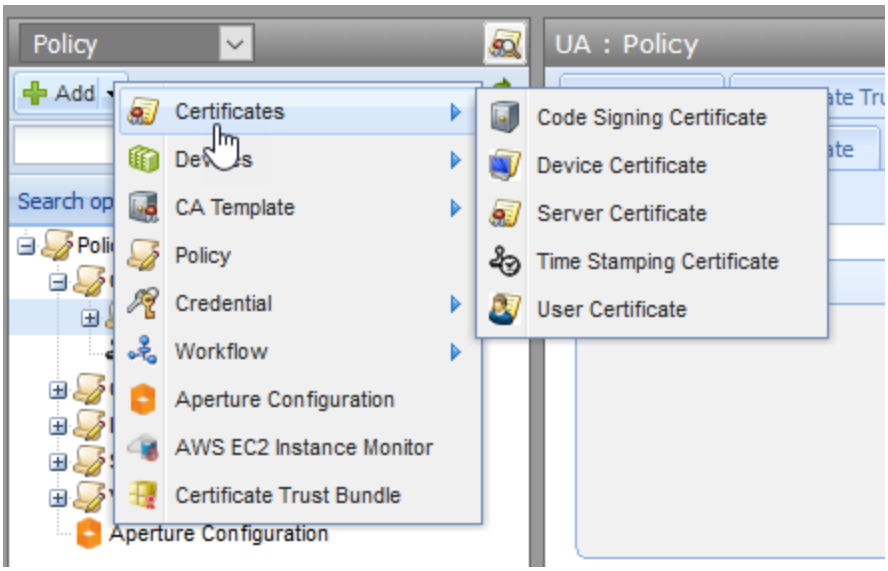
If encryption system assets are managed locally, the organizational folder structure provides a natural framework to distribute your system administration. Object contacts and administrative permissions can be assigned in each locale's folder. For example, the individual responsible to maintain the encryption assets located in Austin, Texas, would be assigned as an object contact and given administrative permissions in the Austin folder object.

If encryption assets are regionally managed, object contacts and administrative permissions can be assigned further up the tree. If centrally managed, the object contacts and administrative permissions can be assigned at the root folder.

Overview of certificate types

In addition to the traditional SSL/TLS (server) certificate, Trust Protection Platform recognizes User certificates, Client Device certificates, and Code Signing certificates.

Each certificate type has its own icon.



BEST PRACTICE Certificate types are important because they let you organize and view your entire certificate population, by type. With four types of certificates, Trust Protection Platform is able to be more selective with new or existing features like validation and provisioning.

When an employee is reassigned or leaves the company, knowing the number and types of certificates they managed or owned is critical.

Finally, running a report that shows you the number of each type of certificate being used by your company helps ensure that your company is in compliance with Trust Protection Platform's licensing requirements.

What's a Server certificate?

SSL certificates are data files that digitally bind a cryptographic key to an organization’s details. Typically, SSL is used to secure, among other things, data transfer and logins.

SSL certificates bind together:

- A domain name, server name, or hostname
- An organizational identity (i.e. company name) and location

In Trust Protection Platform, a certificate is classified as a SSL/TLS if it has an extended key usage (EKU) of Server Authentication.

What's a Code Signing certificate?

A code signing certificate is used to digitally sign software programs as a way for software recipients to verify the authenticity and integrity of the software.

In Trust Protection Platform, a certificate is classified as a code signing certificate if it contains and extended key usage (EKU) of Code Signing.

What's a user certificate?

In Trust Protection Platform, a certificate is classified as a user certificate if it meets the following criteria:

- Does not have an extended key usage (EKU) of Server Authentication or Code Signing
- Is a Smart Card

- SAN Principal = UPN, email, or RFC822
- Subject Type = User

What's a Device certificate?

In Trust Protection Platform, a certificate is classified as a client device certificate if does not meet any of the criteria specified for the previous certificate types.

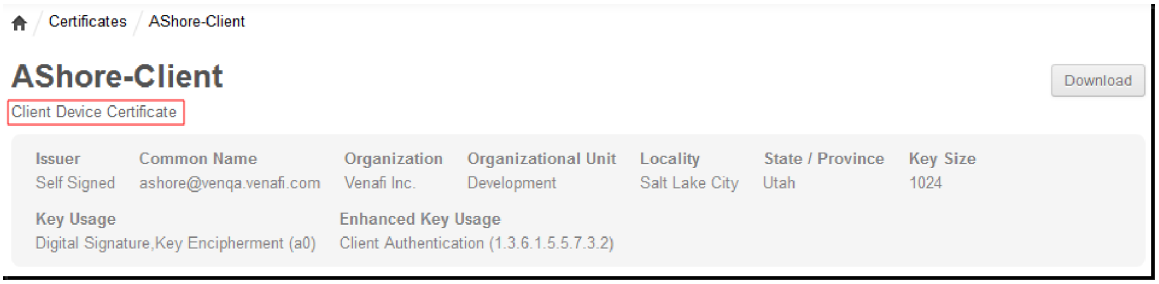
What's a Time Stamping certificate?

In Trust Protection Platform, a time stamping certificate provides RFC 3161-compliant time stamping for code signing. It is used as part of the CodeSign Protect product. For more information about time stamping, see Understanding time stamping in code signing and Using the CodeSign Protect Time Stamp Service.

> **NOTE** The CA/Browser forum has special rules around time stamping certificates. While such a certificate is issued with long (5 or more years) validity, the rules require that the certificate be re-keyed every 15 months. Trust Protection Platform enforces this rule, both for notifications as well as for renewal. This means that a time stamping certificate that is 15 months old will be automatically renewed if set to enrollment. The notifications will be sent according to regular configuration settings, except that they will consider the cert issuance date + 15 months as the expiration. To avoid confusion, notification events for time stamping certificates explain this.
>
> CA/Browser forum rules also require that the key of a time stamping certificate be stored in hardware only. Trust Protection Platform will issue an alert-level notification if the certificate key is stored in software. The Time Stamping settings tab in Policy Tree provides a dropdown allowing you to select where they key should be stored.

What will the different certificates look like?

A certificate type displayed in TLS Protect:

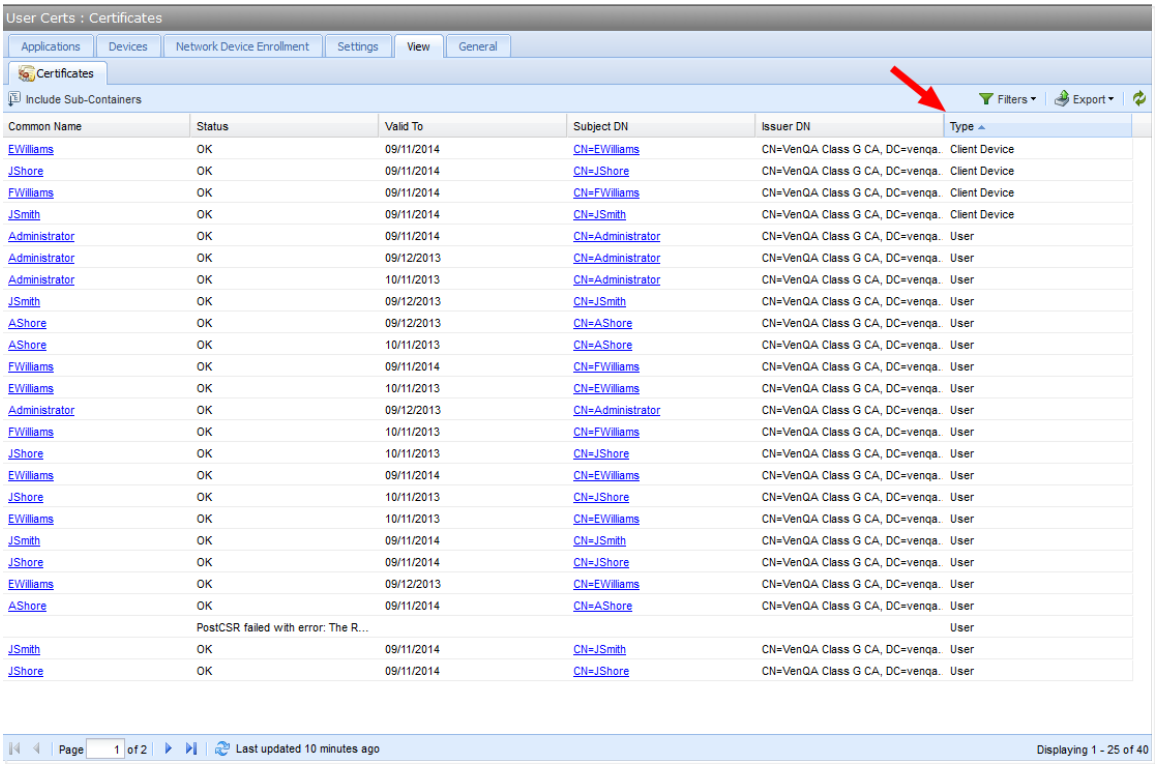


How can I see the different certificate types in my folders?

You can see the types of all certificates under a policy.

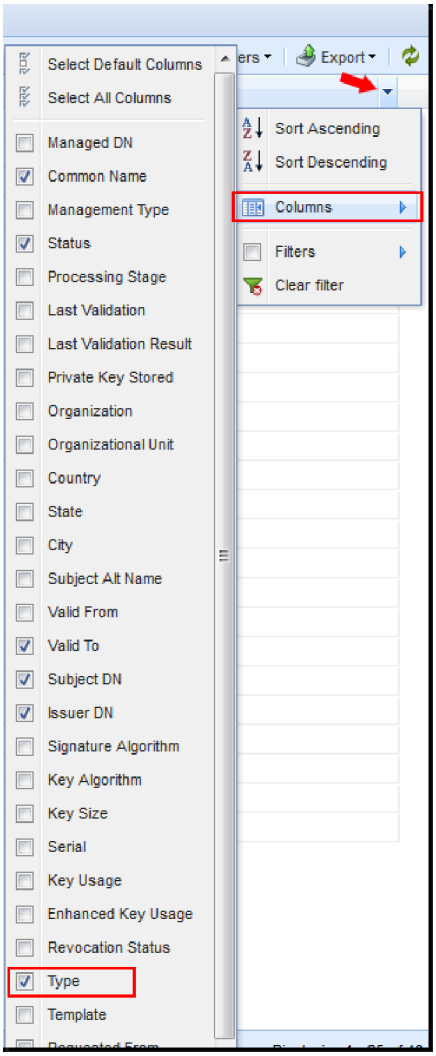
1. In the **Policy** tree, select the policy containing the certificates you want to see.
2. Click the **View** tab.

   You'll see a grid view of the certificates governed by that policy, and their attributes.



If you don't see the column in the grid, you can add it.

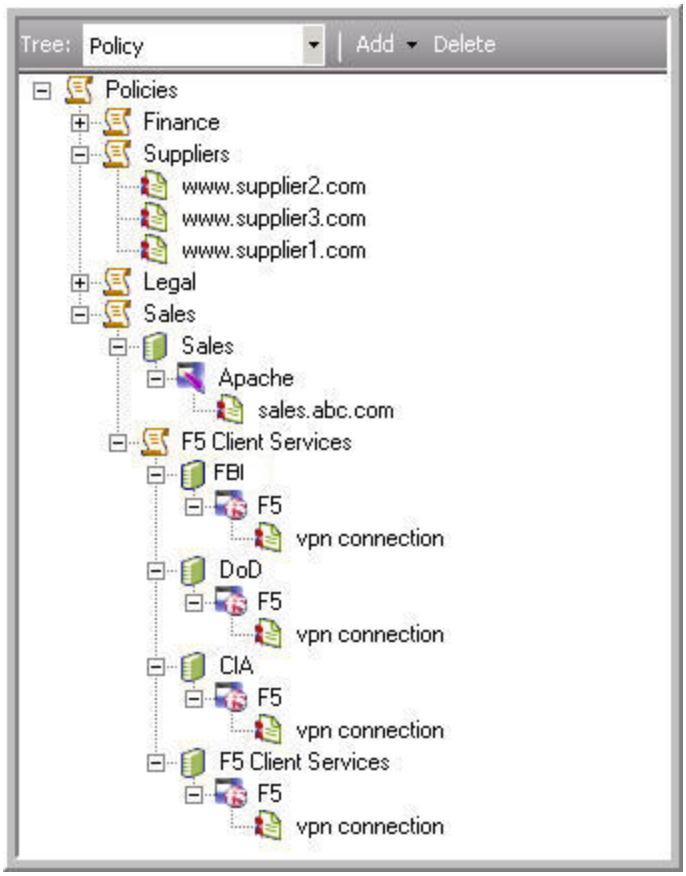
1. Click the drop-down arrow, select **Columns**, then select **Type**.



Using multiple structures

Many organizations have encryption systems that cannot be adequately managed with a single policy structure. They might host internal and external certificates at Monitoring, Enrollment, and Provisioning levels; encryption resources might be distributed by department or division; and multiple applications might support a single URL. In these cases, the most effective way to deploy policies is to leverage multiple policy structures.

The following example leverages a combination of Organizational, Management Level, and Application policy structures.



- The Organizational policy structure is used to group encryption assets by department.
- The Monitoring Level policy structure is used to divide lifecycle management requirements. The Suppliers policy monitors third-party certificates that are critical to the organization's business. The Sales policy, on the other hand, defines parameters for provisioned certificates.
- The Application policy structure is used to enforce consistent configuration parameters for the F5 servers that support client servers. Because the F5 servers support client services for governmental agencies, the F5 Client Services policy locks the **Use FIPS** value so all subordinate servers are FIPS compliant.

  IMPORTANT Because FIPS is not supported for ACMEv2, you cannot have FIPS enabled on any server that is used for ACMEv2.

Managing your policies (folders)

This section outlines how to create and manage policies in your encryption environment. It addresses how policies can be leveraged to support your encryption system infrastructure and standardize certificate deployment and administration.

About policy (folder) hierarchies

Policies—also known as folders—are created and managed in the Folders tree. The Folders tree provides a hierarchical view of your encryption management environment, so you can see folders and their settings.

To access your folders

- From the TLS Protect menu bar, click **Configuration** > **Folders**.

Creating policies

Policies provide a hierarchical framework for managing configuration and assets within your environment, much like hierarchical directories such as Active Directory. Using policies, you apply policy settings which allow you to standardize configuration parameters and enforce security requirements throughout your encryption environment.

To create a policy

1. Log in to Policy Tree.

   IMPORTANT You must have the Create permission on the Policy object where you want to create the new policy.

2. Select the Policy tree from the Tree drop-down menu.
3. In the Policy tree, select the Policy object where you want to create the new policy.
4. Click **Add** > **Policy**.
5. Define the Policy settings.
6. Click Save/**Apply**.

After you create the Policy, you can configure policy settings for the Policy's subordinate encryption objects. The following table describes the Policy configuration settings.

Field	Description
General	
Policy Name	The name of the Policy object.
Description	Description for the Policy object.
Contact	User or Group Identity assigned to the current Policy object. Default system notifications are sent to the contact Identity. To select the Policy Contact: Click the Browse button. The Identity Selector dialog opens. If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, you can enter the wildcard character (*). Select a User or Group Identity, and then click **Select**. Press Shift+click to select multiple, contiguous users and groups. Press Ctrl+click to select multiple, discontiguous users and groups.
Exclude from automatic deletion	When checked, the Recycle Bin's deletion tasks will not be run on objects that use this policy.

Field	Description
	One feature of the Venafi Recycle Bin helps manage the size of your database by automatically deleting old objects that are outdated, based on the settings you configure. However, in cases where certain objects should be protected from deletion, like in a situation where legal obligations require it, you can protect certain objects from being deleted, while allowing the Recycle Bin to run on objects that don't require the same level of protection. To learn more about the Recycle Bin, see "Venafi Recycle Bin" on page 138.
Log View	

Field	Description
Server	The Log View Server provides the current Policy and its subordinate objects with a reference to your Default SQL Channel object. The Default SQL Channel object is the log store for the events used to populate the Log tab within each object configuration. When you install Trust Protection Platform, the root Policy is automatically configured with the default Log View Server object. The Log tab within each object configuration provides a view of all events triggered by the current object. To view events on this tab, you must configure the Log View Database Access credentials in your Default SQL Channel object. For more information, see "Updating the SQL Server channel object" on page 448. To view the log history for the current Policy object, click the Log tab. For more information, see "General configuration options" on page 534.
Processing Engines	
Engines	Allows the administrator to select a specific Trust Protection Platform Server to provide monitoring, provisioning ,and validation services for the Policy's subordinate objects. This functionality is particularly useful in heavily firewalled environments where you want the local Trust Protection Platform server at each site to manage processing for the local certificates and keys. **IMPORTANT** For the CSR generation setting on the certificate: When CSR generation is done by the application: ■ Stages 0 through 400 and 800 and higher use this setting from the policy containing the app. ■ Stages 500 through 700 are done by the policy containing the certificate. When CSR generation is **not** done by the application: ■ Stages 0 through 700 are done by the policy containing the certificate. ■ Stages 800 and higher use this setting from the policy containing the app.

Field	Description

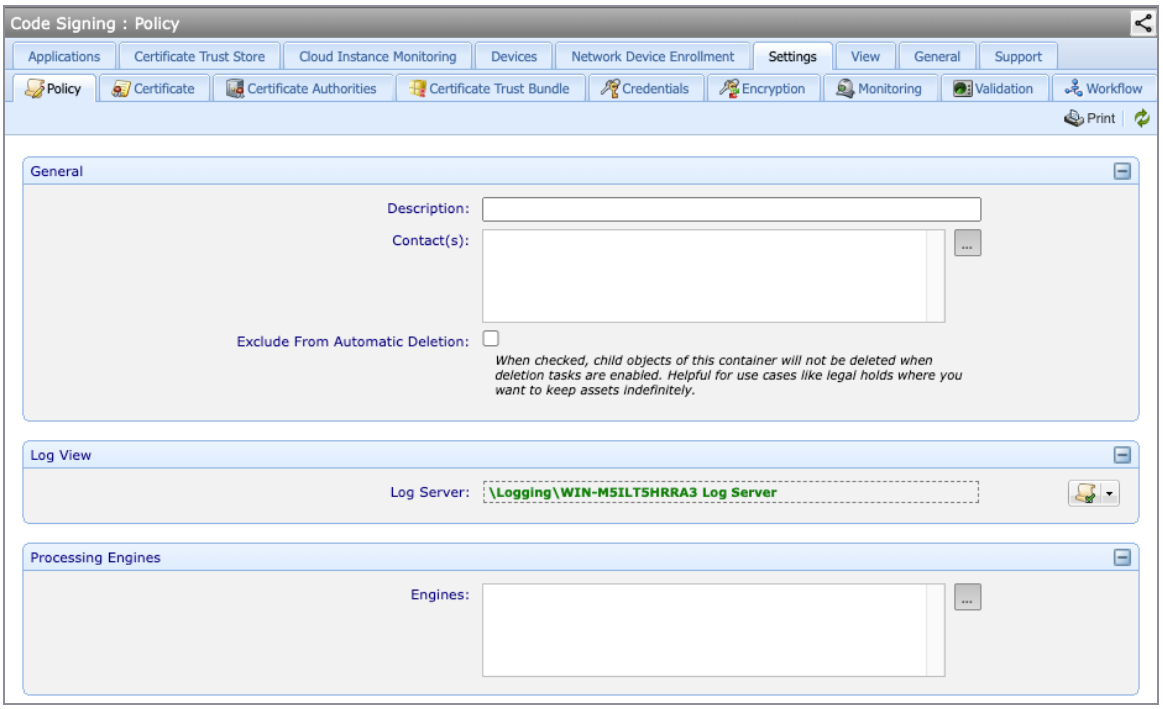
Configuring policies

Policies allow administrators to define global configuration parameters, or “folders,” for the Policy object’s subordinate encryption resources. Each encryption resource in the Policy tree has a corresponding configuration tab within the Policy object.

IMPORTANT You must have the *view* and *write* permissions to the Policy.

To configure a policy (or folder) object using the Policy Tree

1. From the Platform menu bar, click Policy Tree.
2. Select the **Policy** tree from the **Tree** drop-down menu.
3. In the **Policy** tree, select the policy you want to configure.



4. Using the configuration tabs, define the parameters you want to apply to the policy's subordinate objects.

Policy Object Configuration Tabs

Group Tab	Configuration Tab	Description
Applications	The Policy object's Applications tab allows you to define policy settings for subordinate Application objects.	
	Adaptable	Defines policy for subordinate Adaptable application objects. For more information about settings, see Configuring an Adaptable Application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Amazon AWS	

Group Tab	Configuration Tab	Description
	Apache	Defines policy for subordinate Apache application objects. For more information about settings, see Creating an Apache application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Azure Key Vault	Defines policy for subordinate Azure Key Vault application objects. For more information about settings, see in the *Certificate Authority and Hosting Platform Integration Guide*.
	Basic	Defines policy for subordinate Basic application objects. For more information about settings, see Basic application configuration checklist in the *Certificate Authority and Hosting Platform Integration Guide*.
	Blue Coat SSLVA	Defines policy for subordinate Blue Coat application objects. For more information about settings, see Creating a Blue Coat SSLVA application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	CAPI	Defines policy for subordinate CAPI application objects. For more information about settings, see Creating a CAPI application object in the *Certificate Authority and Hosting Platform Integration Guide*.

Group Tab	Configuration Tab	Description
	Citrix NetScaler	Defines policy for subordinate Citrix NetScaler application objects. For more information about settings, see Creating a Citrix NetScaler application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Connect:Direct	Defines policy for subordinate Connect:Direct application objects. For more information about settings, see Creating a Connect:Direct application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	F5 LTM Advanced	Defines policy for subordinate F5 LTM Advanced application objects. For more information about settings, see Configuring an F5 LTM Advanced application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	IBM WebSphere DataPower	Defines policy for subordinate IBM WebSphere DataPower application objects. For more information about settings, see Creating an IBM WebSphere DataPower application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	IBM GSK	Defines policy for subordinate GSK application objects. For more information about settings, see Creating an IBM GSK application object in the *Certificate Authority and Hosting Platform Integration Guide*.

Group Tab	Configuration Tab	Description
	Imperva MX	Defines policy for subordinate Imperva MX application objects. For more information about settings, see Creating an Imperva MX application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	JKS	Defines policy for subordinate JKS application objects. For more information about settings, see Creating a JKS application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Oracle iPlanet	Defines policy for subordinate Oracle iPlanet application objects. For more information about settings, seeCreating an Oracle iPlanet application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Palo Alto Networks Firewall	Defines policy for subordinate Palo Alto Networks Firewall application objects. For more information about settings, see Creating a Palo Alto Networks Firewall application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	PEM	Defines policy for subordinate PEM application objects. For more information about settings, see Creating a PEM application object in the *Certificate Authority and Hosting Platform Integration Guide*.

Group Tab	Configuration Tab	Description
	PKCS#12	Defines policy for subordinate PKCS#12 application objects. For more information about settings, see Creating a PKCS#12 application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Riverbed SteelHead	Defines policy for subordinate Riverbed SteelHead application objects. For more information about settings, see Creating a Riverbed SteelHead application object in the *Certificate Authority and Hosting Platform Integration Guide*.
	Tealeaf PCA	Defines policy for subordinate Tealeaf PCA application objects. For more information about settings, see in the *Certificate Authority and Hosting Platform Integration Guide*.
Devices	The Policy object's Devices tab allows you to define policy settings for subordinate Device and Jump Server objects.	
	Device	Defines policy for subordinate Device objects. For more information about settings, see Managing devices using policiesin the *Certificate Authority and Hosting Platform Integration Guide*.
	Jump Server	Defines policy for subordinate Jump Server objects. For more information about settings, see Managing jump server objects via policy in the *Certificate Authority and Hosting Platform Integration Guide*.

Group Tab	Configuration Tab	Description
Network Device Enrollment		Trust Protection Platform now supports the SCEP protocol. When Network Device Enrollment is configured, Trust Protection Platform can receive a CSR from a SCEP-enabled device, renew the certificate with the appropriate CA, then allow the device to download the renewed certificate from the Trust Protection Platform server. As a non-CA-based certificate enrollment solution for SCEP systems, Trust Protection Platform can manage certificate enrollment with multiple CAs using multiple CA templates. Additionally, Trust Protection Platform provides a robust system of hierarchical, policy-based rules that allow administrators to manage where certificate objects are created in the Policy tree. For more information about settings, see Certificate enrollment via SCEP protocol in the *Venafi Trust Protection Platform Certificate Management Guide*.
Proxy	The Policy object's Proxy tab defines proxy server settings for the CAs that support Proxy server configurations. The Proxy tab is available only in Policy Tree.	
	Entrust Certificate Services CA	Defines proxy settings for subordinate Entrust Certificate Services CA template objects. For more information about settings, see Managing Entrust Certificate Services CA template objects via policy in the *Certificate Authority and Hosting Platform Integration Guide*.

Group Tab	Configuration Tab	Description
	RedHat Certificate System CA	Defines proxy settings for subordinate RedHat Certificate System CA template objects. For more information about settings, see Configuring the RedHat Certificate System CA template object in the *Certificate Authority and Hosting Platform Integration Guide*.
Settings	The Policy object's Settings tab defines proxy server settings for the CAs that support Proxy server configurations.	
	Policy	Defines the Policy description, Contact, Log View server, and Processing Engines. For more information about settings, see the "Creating policies" on page 874. Additionally, there is a setting the prevents items within this policy from being automatically deleted by Recycle Bin tasks. For example, if there is a legal hold and you need to keep assets indefinitely, this setting prevents them from being automatically deleted when otherwise they would due to Recycle Bin settings.
	Certificate	Defines policy for subordinate Certificate objects. For more information about settings, see Managing certificate configuration in the *Venafi Trust Protection Platform Certificate Management Guide*.
	Certificate Authorities	Defines global settings for subordinate CA Template objects.

Group Tab	Configuration Tab	Description
	Credentials	Defines default encryption keys (the default software or custom HSM keys) used to secure certificates, private keys, usernames, passwords, and credentials in the Trust Protection Platform database. For more information, see "To Assign Encryption Keys to Specific Types of Objects in the Policy Tree" on page 575.
	Encryption	Displays the encryption keys used to secure a Policy's subordinate objects. For more information, see "Viewing the Encryption Keys Used to Secure a Policy's Subordinate Objects" on page 576.
	Monitoring	Defines the intervals at which Trust Protection Platform generates expiration events for the Policy object's subordinate Certificate, SSH Server Key, and SSH User Key objects. You can define how soon and how often expiration events are generated for each object type. For more information, see "Configuring expiration event intervals" on page 507.
	SSH Server Key	Defines policy for subordinate SSH Server Key objects.
	SSH User Key	Defines policy for subordinate SSH User Key objects.
	Validation	Disables validation for the policy's subordinate objects based on object type. You can disable validation for each Application object type, SSH Server Key objects, and Certificate objects.

Group Tab	Configuration Tab	Description
		For more information on Certificate and Application object validation, see SSL/TLS network validation in the *Venafi Trust Protection Platform Certificate Management Guide*.
	Workflow	Determines which Workflow objects you want to apply or block to the policy's subordinate Certificate and Application objects. For more information, see Applying or blocking application workflows in the *Trust Protection Platform Certificate Management Guide*. Determines which Workflow objects you want to apply or block to the policy's subordinate Certificate and Application objects. For more information, see Applying or blocking application workflows in the *Trust Protection Platform Certificate Management Guide*.
View		
	Certificates	Lists the policy's subordinate Certificate objects. For more information, seeViewing the Policy's Certificates in the *Venafi Trust Protection Platform Certificate Management Guide*.
	SSH Server Keys	Lists the policy's subordinate SSH Server Key objects.
	SSH Client Keys	Lists the policy's subordinate SSH Client Key objects.

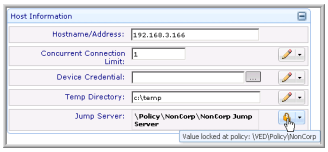
Group Tab	Configuration Tab	Description
General		
	Log Tab	Provides a view of all events triggered for the current object. An administrator must have a minimum of the Read permission to view this tab. For more information on the Log tab options, see "General configuration options" on page 534.
	Permissions Tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

5. Click Save/**Apply** on every tab where you define policy settings.

Configuring a policy's subordinate objects

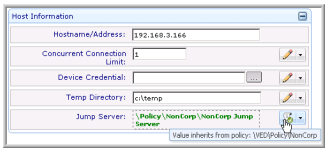
When you create new objects under a policy, locked values are noted with the locked policy icon. These values cannot be changed in objects that are protected by that policy.

When you move your pointer over a locked attribute's icon, a pop-up window shows the parent policy where the locked value is defined.



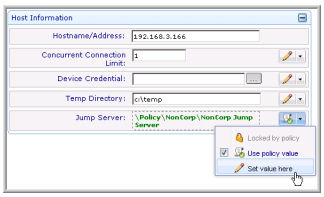
Unlocked policy values can be changed in subordinate objects. When you create a new object under a policy, unlocked policy values display as the object's default configuration. They are noted with an icon, indicating that the value is in compliance with the parent policy. You can either leave the value as it is or override the suggested policy value with your own definition.

When you move your pointer over an unlocked attribute's icon, a pop-up window shows the parent policy where the suggested value is defined.



To override a suggested policy value in Policy Tree

1. Click the attribute's arrow .



2. Click **Set value here**.

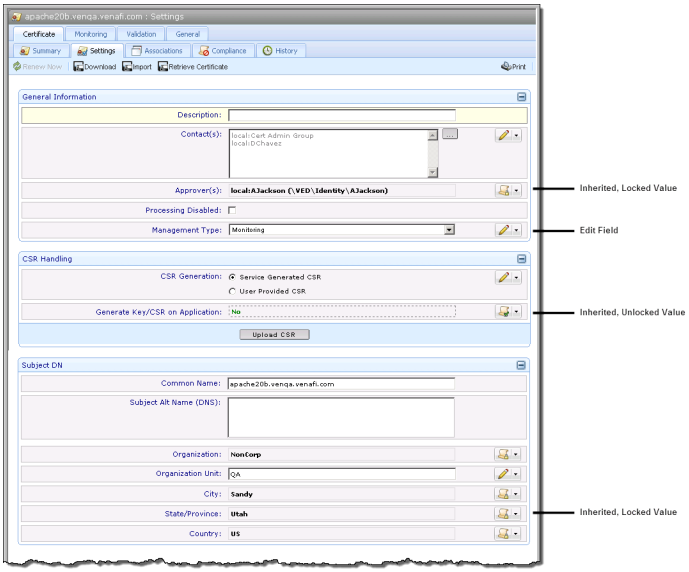
   The attribute's icon changes to indicate the current value is in an edit state .

To override a policy value in Policy Tree

1. Click the icon.

2. Click the icon again to toggle between the policy value and an edit state .

   The following graphic shows the certificate configuration that results from the policy shown on "Locking policy values" on page 863.


apache20b.venqa.venafi.com : Settings
Certificate
Monitoring
Validation
General
Summary
Settings
Associations
Compliance
History
Renew Now
Download
Import
Retrieve Certificate
Print
General Information
Description:
Contact(s):
local:Cert Admin Group
local:DChavez
Approver(s):
local:AJackson (\VED\Identity\AJackson)
Processing Disabled:
Management Type:
Monitoring
CSR Handling
CSR Generation:
Service Generated CSR
User Provided CSR
Generate Key/CSR on Application:
No
Upload CSR
Subject DN
Common Name:
apache20b.venqa.venafi.com
Subject Alt Name (DNS):
Organization:
NonCorp
Organization Unit:
QA
City:
Sandy
State/Province:
Utah
Country:
US
Inherited, Locked Value
Edit Field
Inherited, Unlocked Value
Inherited, Locked Value

17

Working with custom fields

Custom Fields give you a way to extend Trust Protection Platform's out-of-the-box capabilities to capture data points that are not part of the standard trust protection lifecycle and may be unique to your environment.

Being able to store additional data allows Trust Protection Platform to become more tightly aligned with your internal business processes without requiring any custom software development. Custom fields can also be used to correlate Trust Protection Platform objects with non-Trust Protection Platform infrastructure whether it's a manual process or integration between applications.

The ability to add custom fields gives you:

- A place to store arbitrary data related to assets that Trust Protection Platform is already tracking
- A way to better align Trust Protection Platform with customer-specific business processes
- A basis for correlating Trust Protection Platform assets with external infrastructure
- A way to collect additional data from certificate managers about their assets

EXAMPLE Let's say that you want to be able to track your certificates by Location or Cost Center. You can create custom fields called *Location* and *Cost Center* that can be applied to certificates or devices. When you need to, you can export the data or view a report that shows you certificates and devices that use Location and Cost Center.

NOTE Only Venafi's Symantec Managed PKI for SSL and Entrust Certificate Services drivers support vendor custom fields. If you want to use custom fields, we recommend using Venafi's custom fields feature. To ensure a smooth ride, either ensure that all custom fields for your chosen vendor are *optional* and use Venafi's custom fields instead, or use one of Venafi's custom field-supported drivers (Symantec or Entrust).

This chapter contains the following topics:

Adding or deleting a custom field 893

Editing a custom field 900

Filtering custom fields 901

Viewing custom fields 902

Generating a Custom Fields report 903

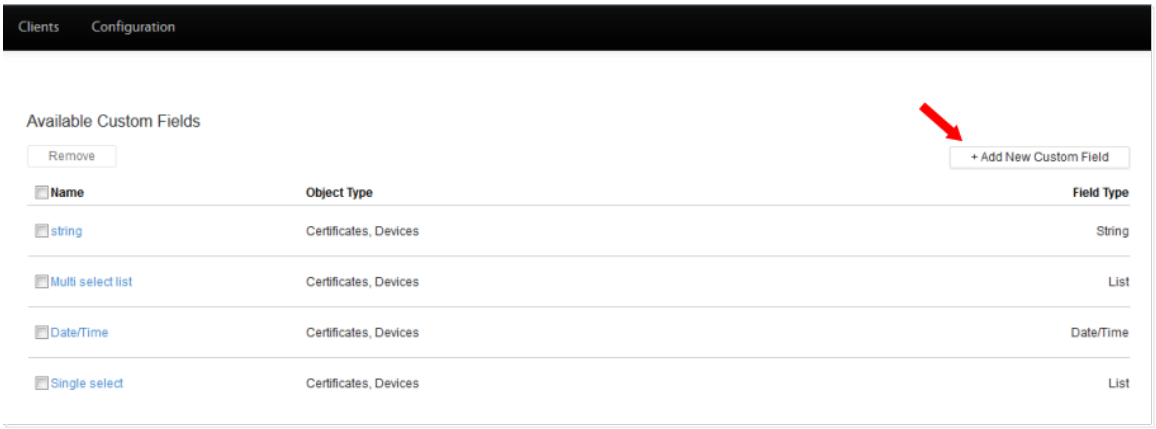
Using the Custom Field macro for notifications 905

Adding or deleting a custom field

After adding or deleting a custom field, you must restart IIS for the changes to be visible in Aperture.

To add a custom field

1. From the menu, click click **Configuration** > **Custom Fields**.
2. In Available Custom Fields, click **+Add New Custom Field**.

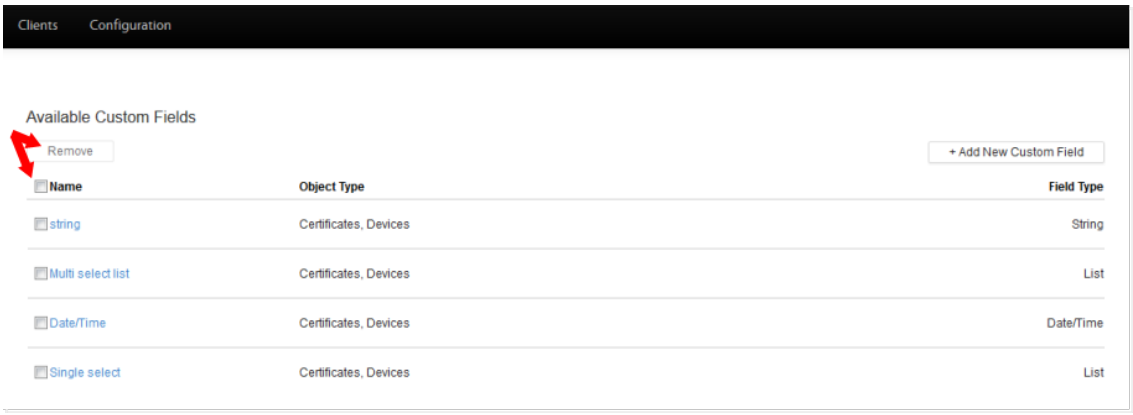


3. Configure the new Custom Field. See "Custom field configuration settings" on the next page
4. When you're done, click **Save**.

To delete a custom field

When you delete a custom field, all data associated with that field will also be deleted.

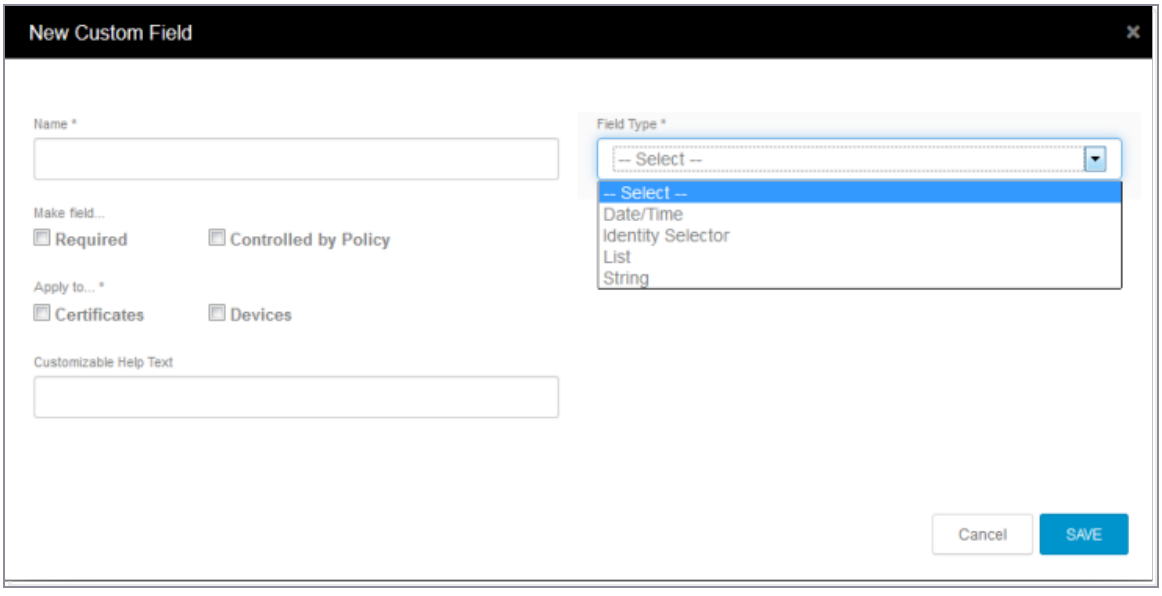
1. From the TLS Protect menu bar, click click **Configuration** > **Custom Fields**.
2. In Available Custom Fields, select the custom field you want to delete.



3. Click **Remove**.
4. When asked, if you're sure you want to delete the field, click **Delete**.

Custom field configuration settings

Here are the configurable settings for a new custom field.



Name (Required)

Enter the name of the new custom field.

Make field...

Required

The field is required on every object. The object can't be saved unless this field has been completed.

Controlled by Policy

The field inherits the settings of the policy under which the object is placed.

HIdden

The field is not shown in the following places:

Console	Not displayed
Policy Tree	Certificate > Settings tab
Policy Tree	Policy > View > Certificate grid
Policy Tree	Device > Settings tab
Aperture	Certificate Renewal Details (view or edit)
Aperture	Certificate inventory list view
Aperture	Device details Edit device settings

Read only

The field is read-only in the following places:

Console	Displayed but not editable
Policy Tree	Certificate > Settings tab
Policy Tree	Policy > View > Certificate grid
Policy Tree	Device > Settings tab
Aperture	Certificate Renewal Details (view or edit)
Aperture	Certificate inventory list view
Aperture	Device details Edit device settings

Apply to... (Required)

Choose one or more:

- Certificates
- Devices

Customizable Help Text

Create your own text that will help your users determine which settings to choose.

Field Type (Required)

A field type cannot be changed after the custom field is created. You must delete the custom field then create a new one.

Select a field type from the drop-down list:

- Date/Time (in 15 minute increments)
- Identity Selector
- List

See "Creating a single or multi-select list in a custom field" below.

- String - create a string-based field that can be validated

Validation Template (string-based custom fields)

Create a string validation template using regular expressions.

Validation Regular Expression

Review or change the suggested regex.

Validate Sample Entry

Type in a sample entry to validate regular expressions..

= Invalid regular expressions

= valid regular expressions

Customizable Error Message (for String Field Type only)

Create a customized error message to display when an entry or selection is incorrect.

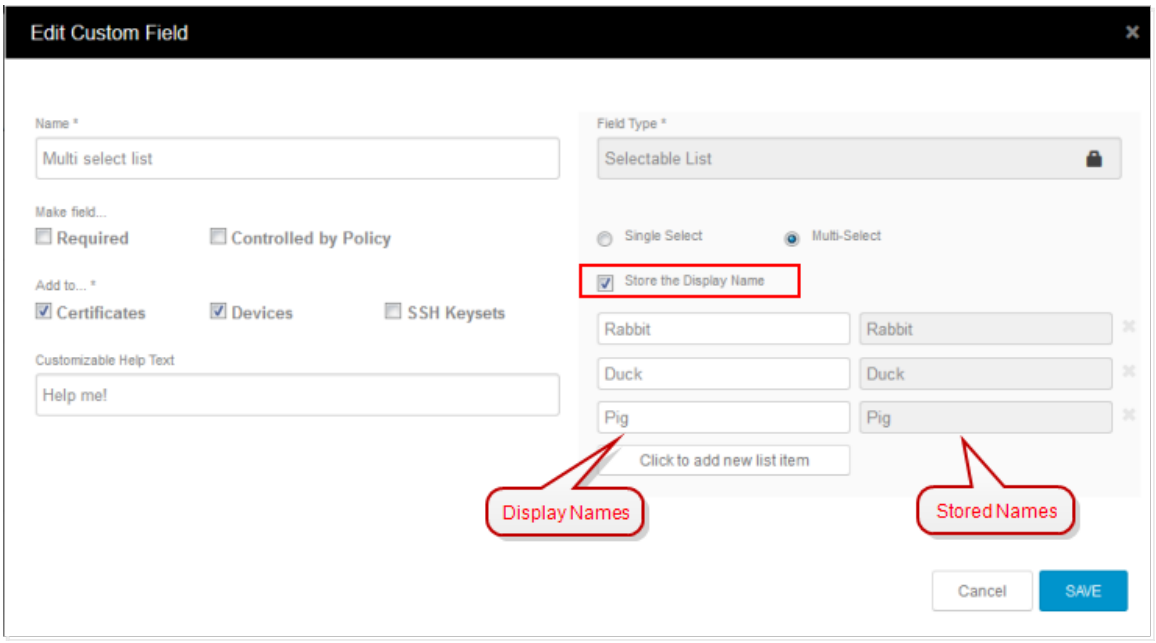
Creating a single or multi-select list in a custom field

You can create a single or multi-select list to apply to objects.

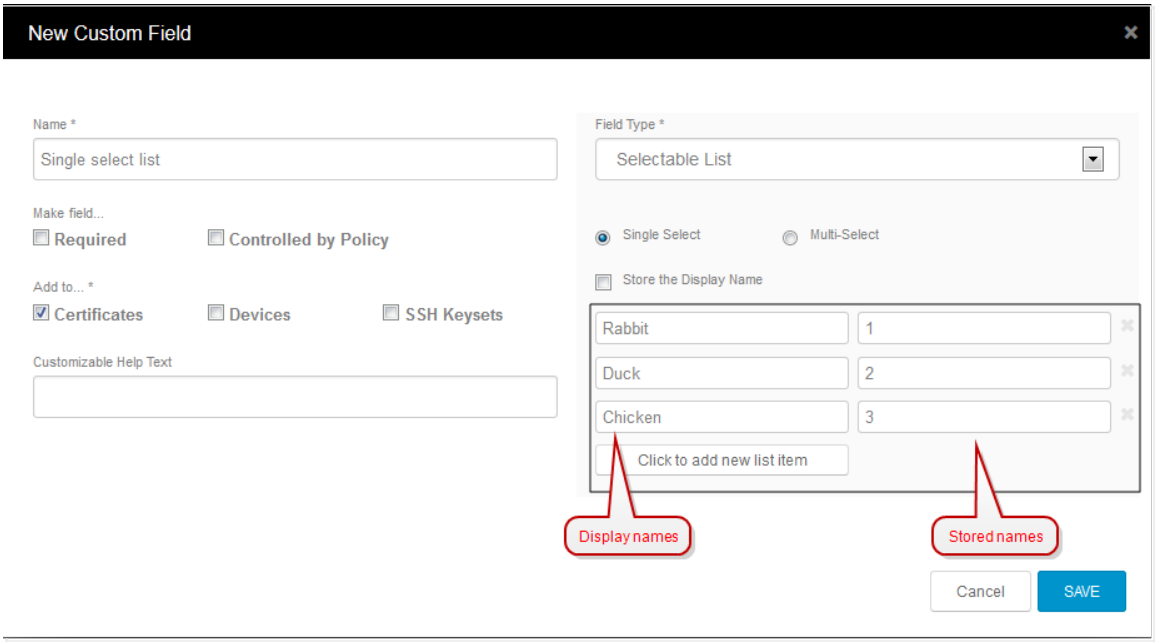
To Create a single-select list

1. From the menu, click **Configuration** > **Custom Fields**.
2. In Available Custom Fields, click **+Add New Custom Field**.
3. From the **Field Type** drop-down list, choose **List**.
4. Choose **Single Select**.
5. Enter a Display Name.

6. If you want the Display Name to be recorded in the database, select the check box **Store the Display Name.**



7. If you want to specify something other than the Display Name to be recorded, clear the check box then enter the stored name.

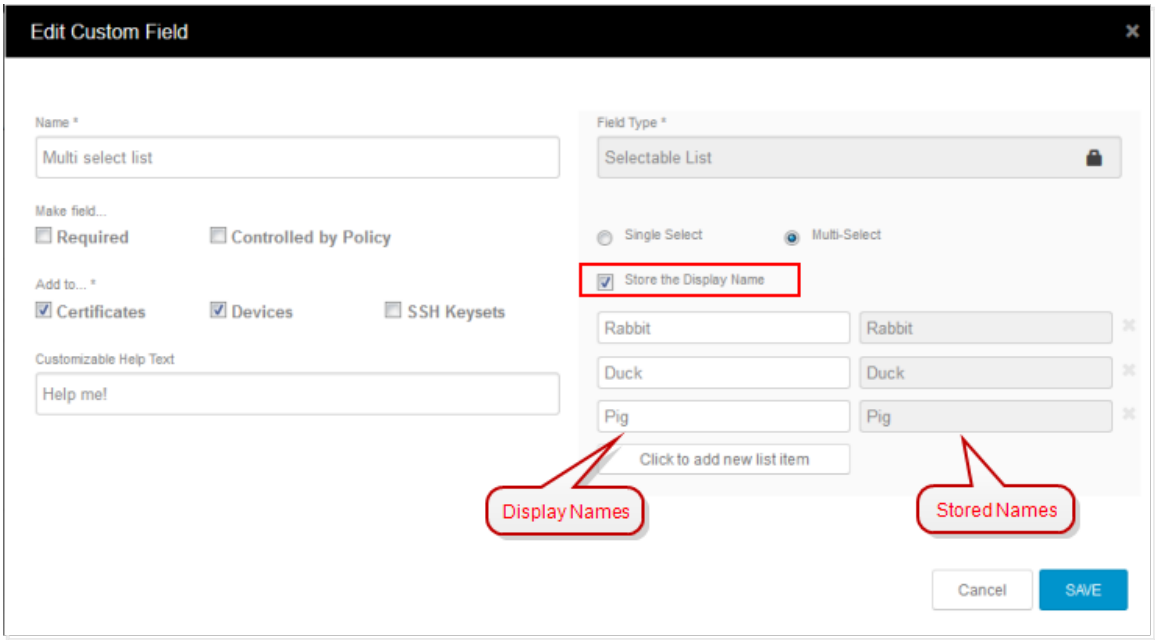


8. When you're done, click **Save**.

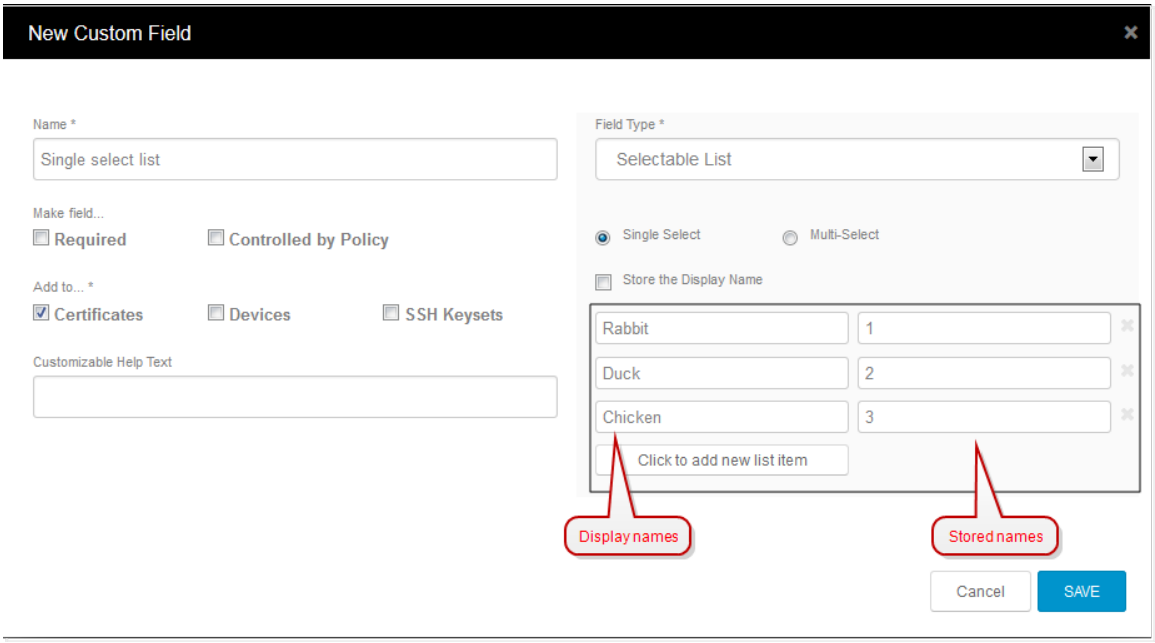
To Create a multi-select list

1. From the TLS Protect menu bar, click **Configuration** > **Custom Fields**.
2. In Available Custom Fields, click **+Add New Custom Field**.
3. From the **Field Type** drop-down list, choose **List**.
4. Choose **Multi-select**.

   If you want the Display Name to be recorded in the database, select the check box **Store the Display Name.**



5. If you want to specify something other than the Display Name to be recorded, clear the check box then enter the stored name.

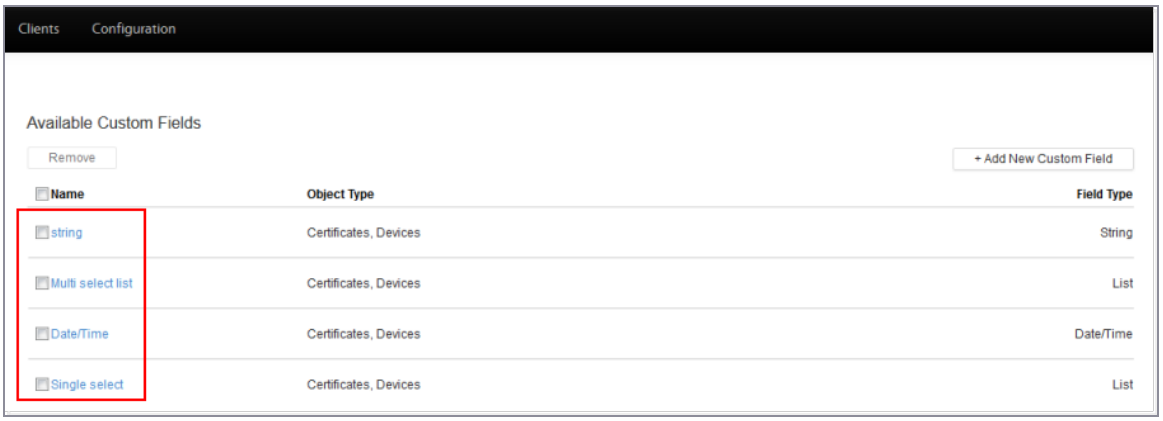


6. When you're done, click **Save**.

Editing a custom field

To edit a custom field

1. In the menu bar, click **Configuration** > **Custom Fields**.
2. In Available Custom Fields, click the custom field you want to edit.



3. In the **Edit Custom Field** window, make changes as needed.

4. Use caution when editing an existing custom field. Changing settings may result in saved data becoming inaccessible.

   To learn more, see Use Caution When Editing a Custom Field.

5. When you're done, click **Save**.

Filtering custom fields

Custom fields can also be used to find items in the same way you can use other filters, allowing you to narrow the list of discovered items.

Custom fields are listed in the Certificate Properties filter group.

To filter items using custom fields in Aperture

1. From the menu, click **Inventory** > **Certificates**.
2. Use filters to narrow your search results.

   As you select and remove filters, the objects list is automatically refreshed giving you instant filter results.

3. Locate the custom filter, which is usually near the bottom of the Certificate Properties filter group list, and apply one or more filters to narrow the list of discovered items.
4. Some custom filter types allow you to select multiple values.

   > **EXAMPLE** When you create a list-type custom field, you can allow users to select multiple items. When you select multiple items in a filter, they are evaluated with an OR expression. Iif the custom field type is *identity selector*, you can select multiple users in your filter, and you will see results for either identity.

   When you use multiple fields for filtering, those are evaluated with an *AND* expression.

   > **EXAMPLE** If you filter on a custom identity type field with a value of *George Washington* and you also filter on a string filter type with text *Customer*, you will only see results that match *both* of these filters.

5. When you find the object you want, click its name to view details.

For more information on filtering in Aperture, see Finding assets in Aperture using filters (Certificate Inventory).

Viewing custom fields

Custom field data appears like normal data in Trust Protection Platform. In table views, you can add the custom fields as columns. On individual objects the custom fields are displayed on the details page.

To view custom fields for every certificate

You can view your custom fields in the certificates grid view of the Policy Tree.

1. Open the Policy Tree.
2. Click on the policy for which you want to see all certificates and their custom fields.
3. Click **View**, and then click **Certificates**.
4. Each custom field has its own column. If a certificate has custom fields associated with it, they will appear in the same row as the certificate.

To view custom fields for an individual certificate

1. In the menu bar, click **Inventory** > **Certificates**.
2. Find the certificate for which you want to enter custom field data.

   See Finding assets using filters on the Certificate Inventory list in the *Trust Protection Platform Certificate Management Guide*.
3. At the certificate details screen, click the **Actions** button, then click **Renewal Details**.
4. In Requested Renewal Details, click **Edit**.
5. In **Renewal Details**, the custom fields appear at the bottom of the window.

To view custom fields for devices

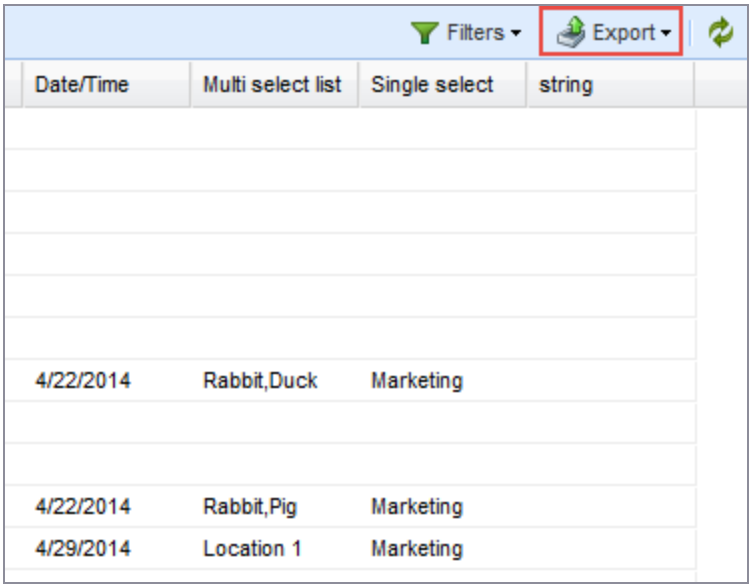
1. Click **Inventory** > **Devices**.
2. Find the device for which you want to enter custom field data.
3. Click the device's name.
4. You'll see the details about the device, including its custom fields.

Generating a Custom Fields report

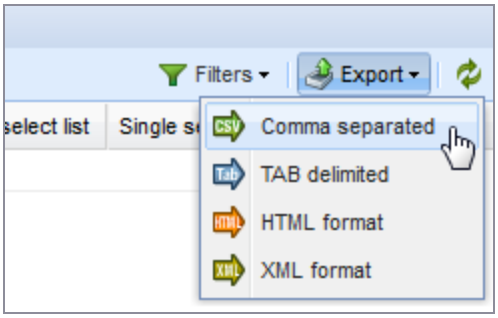
Export custom field information from the Trust Protection Platform to Microsoft Excel or other reporting software.

To generate a custom fields report

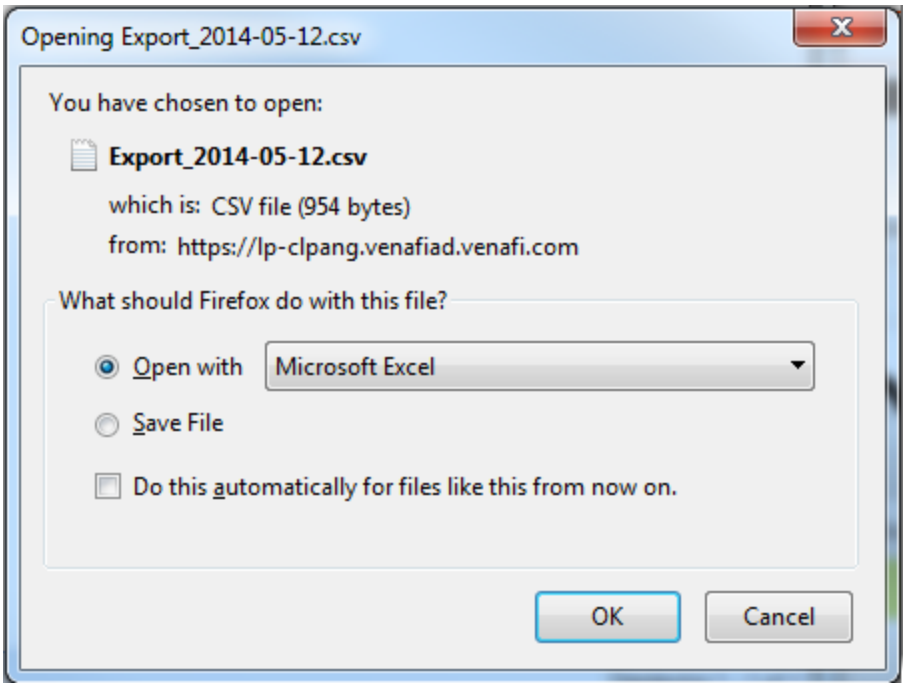
1. In View Certificates, click **Export**.



2. Select **Comma Separated**.

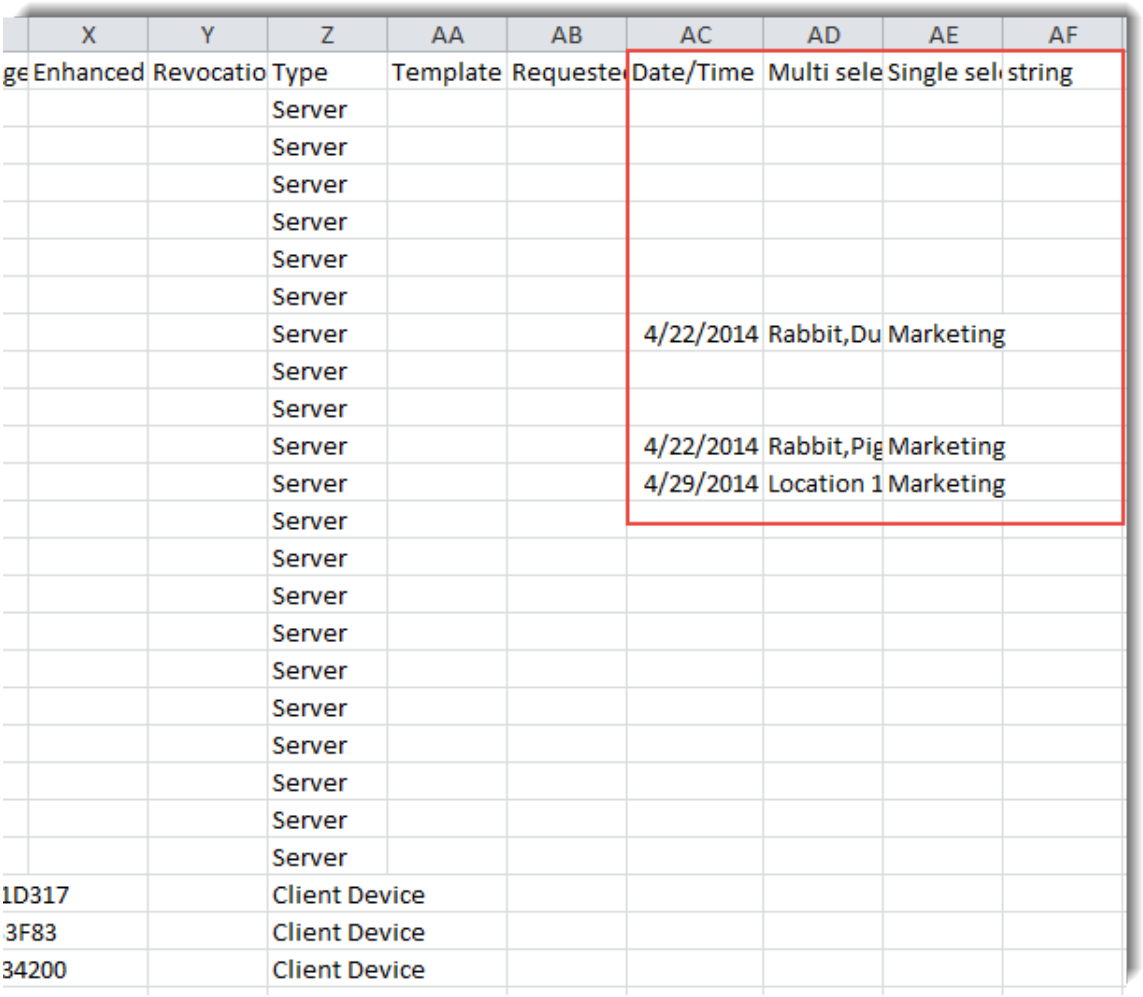


3. In the Opening Export window, you can save the file or open it with the program of your choice. In this example, the data is being exported to Microsoft Excel.



4. Click **OK**.

Here is a snippet showing what the MS Excel report might look like, including custom fields.



	X	Y	Z	AA	AB	AC	AD	AE	AF
ge	Enhanced	Revocatio	Type	Template	Requeste	Date/Time	Multi sele	Single sel	string
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
			Server			4/22/2014	Rabbit,Du	Marketing	
			Server						
			Server						
			Server			4/22/2014	Rabbit,Pig	Marketing	
			Server			4/29/2014	Location 1	Marketing	
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
			Server						
1D317			Client Device						
3F83			Client Device						
34200			Client Device						

Using the Custom Field macro for notifications

Basic macro

The syntax of the basic Custom Fields macro looks like this:

```
$CustomField[<object dn>,<custom field label>]$
```

- **object dn** (distinguished name) is a string like \VED\Policy\Certificates\www.venafi.example representing either a device or certificate object.
- **custom field label** is the label used to uniquely identify the field on the configuration in Aperture and when the field appears on device and/or certificate object.

EXAMPLE If the following macro appears in the message body of a notification that was triggered by an event being logged for a certificate, it would return the effective value for the *Cost Center* custom field:

```
$CustomField[$Event.Component$,Cost Center]$
```

Example output:

```
ABC123
```

IMPORTANT If the data that you are storing in your custom field contains a comma, the Custom Field macro will automatically escape those commas with a backslash character. This allows the Custom Field macro to be nested in other macros. However, if you do not want the commas to be escaped (for example, a comma-separated list of email addresses), you can use the following syntax to **prevent** escaping the data within a stored value.

```
$CustomField[$Event.Component$,Single Value Field,'']$
```

Macro for multiple stored values

The syntax of the multiple stored values macro looks like this:

```
$CustomField[<object dn>,<custom field label>,<delimiting characters>]$
```

If the custom field is capable of storing more than one value (the identity selector, or list with multiple values enabled), you can't output those values as a list. To do that, add a parameter that identifies an escape character, typically the backslash (`\`), and a delimiter, typically the comma (`,`).

This is useful if, for example, you want to modify the Recipients field of an SMTP channel in order to send email to all of the Escalation Contacts (which is the name of the custom field in the example below).

EXAMPLE This syntax returns a comma separated list of *Escalation Contacts* expressed as prefixed universals so they can be fed directly into the IdentityEmail macro to get a comma separated list of their email addresses:

```
$IdentityEmail[$CustomField[$Event.Component$,Escalation Contacts,",\"]$]$
```

Example output:

```
paul@cyberark.example,susan@cyberark.example,carlos@cyberark.example
```

Macro for making a multi-select list human readable

For a multi-select list, you may want to output the information in human-readable form. An optional parameter is available for specifying the word (or symbol) used to join the last item to the rest of the list (a conjunction).

```
$CustomField[<object dn>,<custom field label>,<escape/delimiting chars>,<conjunction>]$
```

EXAMPLE If you have a multi-select list custom field called *Remedy Groups* that allows a user to select zero or more predefined items, you would use the following macro to output it as a human readable comma separated list:

```
$CustomField[$Event.Component$,Remedy Groups,",\","and"]$
```

Example output:

```
Application Support, Windows Servers and Unix Servers
```

Macros for use with Workflows

- Use in a Workflow Reason Code Description field assuming that the workflow only applies at stages involving a certificate object:

  ```
  $CustomField[$Event.Component$,Enterprise Application ID]$
  ```

- Use in the Approver Macro field of a Workflow object (which only accepts identities):

  ```
  $CustomField[$SelfDN$,Escalation Contact,",\"]$
  ```

- Use in the Injection Commands field of a Workflow object (which only applies to application objects, therefore you must first retrieve the distinguished name of the certificate object assigned to the application object from the *Certificate* attribute and then obtain the custom field value of the certificate):

  ```
  $CustomField[$Config[$SelfDN$,Certificate]$,Operating Environment]$
  ```

18

Working with system credentials

In Trust Protection Platform, *credential objects* provide an innovative way to centrally manage and share your system credentials. Each credential object can be associated with a single device or application, or it can be shared by multiple objects.

Most credential objects store the credentials used by Trust Protection Platform to authenticate with devices, applications, CAs, and Active Directory user directories. Without them, Trust Protection Platform can't manage the certificates associated with devices, applications, and CAs. Other Credential objects don't store credentials but instead connect with external password vaults such as CyberArk or HashiCorp Vault (which can be done using the Adaptable Credential).

You create credential objects in Trust Protection Platform using any of the following credential types:

- Adaptable Credential (*Username/Password*, and *Password*)
- Amazon Credential
- Certificate Credential
- CyberArk Username Private Key Credential
- Generic Credential
- Google Cloud CA Credential
- Password Credential

- Private Key Credential
- Username Password Credential

DID YOU KNOW? The actual credential types you see depends on the products you have licensed.

One of the great things about credential objects is that after you create them, you don't have to repeat the credential configuration for every device, application, or CA. You just reference the existing credential object. If the credential changes–for example, an organization's security policy might require changing user name and password credentials every 90 days; or you might need to swap out a private key used by an existing private key credential–you merely update the single credential object to give Trust Protection Platform access to all of its associated devices and applications.

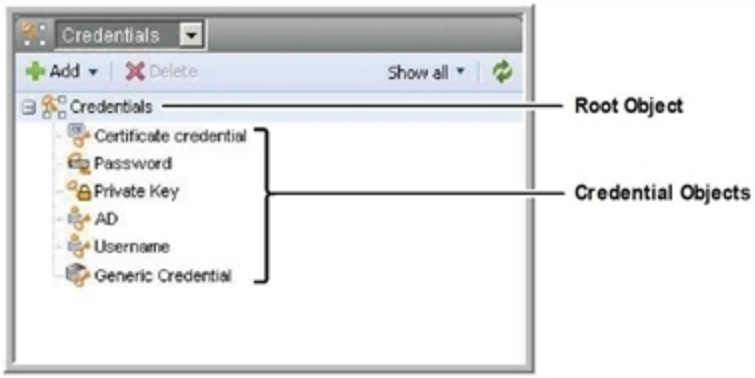
This chapter contains the following topics:

About credential object hierarchy 911
About securing credential objects 911
About credential objects 912
Creating new credentials 912
Managing existing credentials 929
About Amazon credentials 940
Using CyberArk with Trust Protection Platform 944
PowerShell script reference for Adaptable Credential 966
About Generational Management 974

About credential object hierarchy

Credential objects can be created and managed in both the Credentials and Policy trees.

To access credential objects in the Credentials tree, select **Credentials** from the Tree menu. In the Credential tree hierarchy, all Credential objects are created under the Root Credential object.



To access credential objects in the Policy tree, select folders from the Tree menu. To just see credentials on the Policy tree, use the **Filter** drop-down and click **Credentials**.

In the Policy tree hierarchy, Credential objects may be contained by Policy, Device, or Application objects. The ability to create Credential objects under different objects in the Policy tree facilitates the distribution of Credential object permissions assignments. For example, if you assign permissions at the policy level, then create the Credential objects under the same policy where their associated applications or certificates are located, the credentials automatically inherit the same permissions as their associated objects. In this way, you can ensure that administrators have permissions to only those credentials required to manage the applications or certificates for which they are responsible.

About securing credential objects

Every credential object in the Trust Protection Platform database is secured with an encryption key. Trust Protection Platform uses either a software encryption key or a hardware encryption key on a supported HSM (or both) to encrypt your system credentials.

For more information, see "Managing system encryption keys" on page 545.

About credential objects

Under certificate enrollment and provisioning, every CA template must reference the credential required to authenticate with a certificate authority (CA). Devices and applications also require credentials so Trust Protection Platform can authenticate with the device or application during provisioning and onboard validation operations.

You can create credential objects from the Credentials inventory pagen.

See "Creating new credentials " below.

NOTE To create new credential objects, you must have the View, Write, and Create permissions under the Credential or Policy tree where you plan to create them.

Creating new credentials

You can create certificate, username, password, private key, CyberArk and Amazon credentials that Trust Protection Platform can use to authenticate to devices or applications over SSH.

NOTE To create new credential objects, you must have the View, Write, and Create permissions for the folder where you plan to create them.

In Aperture, permissions are controlled in the **Permissions** panel. For information about working with permissions in Aperture, see "Assigning permissions to objects" on page 730.

NOTE Amazon, Google, CyberArk and Adaptable credentials require additional configuration settings.

- For Amazon credentials, see "About Amazon credentials" on page 940.
- For Google credentials, see Setting up Venafi for use with Google Cloud CA Service.
- For CyberArk credentials, see "Adding and configuring CyberArk credentials" on page 958.
- For Adaptable Credentials, see "Creating Adaptable Credentials" on page 921.

To create a new credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select the type of credential you want to create.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
5. Depending on the credential type you selected (in Step 3), you'll need provide additional configuration settings.

   For specific configuration settings for each credential type, refer to the following topics:

   "Creating user name or password credentials" below

   "Creating private key credentials" on page 916

   "Creating certificate credentials" on page 918

   "About generic credential object configuration settings" on page 925

Creating user name or password credentials

User name or password credentials let you store a single user name and password pair that can be used to authenticate to a device, application, or certificate authority (CA).

A password credential lets you to store a single password that can be used to access a keystore or private key, download certificates from a CA, or access any other password-protected object.

To create a username credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Username**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.

5. In **Edit Credential Settings**, in **User Name**, type the username that is part of the credential pair to be stored in Trust Protection Platform where it can be used to connect to your target device, CA, etc.
6. In **Password** and **Confirm Password**, type (and then retype) your password.
7. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
8. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

   The default contact is the master administrator.

   For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.
9. When you're finished, click **Save**.

To create a password credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Password**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
1. In **Edit Credential Settings**, in **Password** and **Confirm Password**, type (and then retype) your password.
2. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
3. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

The default contact is the master administrator.

For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.

1. When you're finished, click **Save**.

Creating a User Name or Password credential using Policy Tree

TLS Protect is the preferred method for creating credentials. However, you can create credentials using the Policy Tree.

To create a user name or password credential using the Policy Tree

1. Open the Policy Tree.
2. From either the **Policy** or **Credentials** tree, right-click the folder where you want to create the new private key credentials, and then click **Add** > **Credential**, and then click either **Username Credential** or **Password Credential**.
3. In **Credential Name**, type a unique name for the new credential object.
4. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
5. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

   The default contact is the master administrator.

   For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.
6. Click **Expires** and select a date when the credential expires.

   IMPORTANT This expiration date is only used to send a log notification. Trust Protection Platform continues to use the credential even if it is past its expiration date.
7. (Conditional) If you're creating a user name credential, then in **User Name**, type a user name for your new credential.

8. In **Password** and **Confirm Password**, type the password associated with the credential.
9. Click **Save**.

Creating private key credentials

A *private key credential* lets you store a private key which can be used for public/private key authentication. Private key credentials are commonly used to authenticate with devices or applications over SSH.

Supported key formats (in either PEM or Putty format) are:

- RSA
- DSA
- ECDSA
- ED25519

When you create a new private key credential, you'll copy and paste the entire contents of your private key file into Aperture, being careful not to add or remove any portion of the contents.

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOQIBAAJBAIOLepgdqXJ5gSA12jcjBrM07O4dV/neBXK5mZO7Gc778HuvhJi+
Rv2EuN9sHPx1iQqqhSi8aCuXuS1vpQJATRDbCuFuqvYiUCAwEAAd2EbFxGXNxhjL
loj/Fc3a6UE8GeifbCAQsptSPIT5vhcudZgWFoeydDUIJjWEMDSXrIn79nXvyPy5
BQIhAPU+XwrLGy0Hd4Roug+9IRMrlu0gtSvTJRWQ/b7m0fbfAiEAiVB7bUMynZf4
SwVJ8NAF4AUxnPjEp8D23sCIA3ZcNqWL7myQ0CZ/W/oikBmYxOJPGVcQzhwkDbck
3GJEZuAB/s9BuKgkCdhlrtIM6/7E+y1p++VU6bh2+vd3AiASmnvOZmI8Zwlgf4Qh
u+zYCJfljtJJpH1IHZW+A60iThKtezaCk7FiAC4=
-----END RSA PRIVATE KEY-----
```

In this example, you'd copy everything from -----BEGIN RSA PRIVATE KEY----- down through -----END RSA PRIVATE KEY-----.

```
PuTTY-User-Key-File-2: ssh-ed25519
Encryption: none
Comment: ed25519-key-20200313
Public-Lines: 2
AAAAC3NzaC15AAAAIM25yKbNXPlZDI1NTETGRZxFkSjyu71LmjYNWctZjUaZgDQb
XoKd
Private-Lines: 1
AAAAIHSoRtc/JPIDUZwBHs3Pq0ykTJM1V8gg+P3Z96Z6Vi+s
Private-MAC: 61f8b9e52e3238feb16e04fb3bfa400bd2ec8334
```

TIP Before you begin, locate and open your private key file in a text editor so that you can copy and paste it's contents in Aperture during the following procedure.

To create a private key credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Private Key**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
5. In the **Edit Credential Settings** box, type the username that's associated with the private key you'll use to create your new private key credential.
6. (Conditional) If you're using an encrypted private key, then in **Password for Private Key**, type the associated password.
7. In **Private Key File Contents**, copy and paste the entire contents from your private key file, making sure that you *copy all of it's contents*.

   See "Creating private key credentials" on the previous page.
8. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
9. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

   The default contact is the master administrator.

   For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.
10. When you're finished, click **Save**.

If at some point you need to replace the private key applied to a private key credential, see "Replacing a private key credential's private key" on page 938.

Creating certificate credentials

The certificate credential feature lets you store private keys that can be used for authentication.

The certificate you select must have a corresponding private key stored within Trust Protection Platform.

> **TIP** Before you proceed, you should know that Aperture only lets you select existing certificates, while Policy Tree lets you either select existing certificates or import a new certificate if the certificate you need is not yet in Trust Protection Platform.

To create a certificate credential (Aperture)

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Certificate**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
5. In **Edit Credential Settings**, click the **Certificate** field to locate and select the certificate to use for this credential.

   The certificate you select must have a corresponding private key stored within Trust Protection Platform.
6. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
7. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

   The default contact is the master administrator.

   For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.
8. When you're finished, click **Save**.

Creating Amazon credentials

You create Amazon credentials the same way you create other credential types. But it's helpful to consider a few things first.

First things first

Before you get started, consider the following:

- Know which authentication method you plan to use: Local, ADFS, or EC2 Assigned Role. For more information, see "About Amazon credentials" on page 940.
- Do you plan to use your new credential across multiple accounts ("cross-accounts")?
- If you haven't already, create a user name credential for use with your new Amazon credential. You can do this during the following procedure, but having it created ahead of time will be faster.
- Make sure you have View, Write, and Create permissions to the folder where you plan to create your new credential object.

> **DID YOU KNOW?** In Aperture, permissions are controlled in the **Permissions** panel. For information about working with permissions in Aperture, see "Assigning permissions to objects" on page 730.

To create an Amazon credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Amazon**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
5. Click the **Source** list and select *Local*, *EC2 Assigned Role*, or *ADFS*, depending on which authentication method you need.
6. (Conditional) If you selected **Local** from the **Source** list, then do the following:

a. Type a password in the **Access Key** and **Secret Key** fields, respectively.

   You'll be required to retype them in each of the confirmation fields.

b. (Optional) If you plan to use this new Amazon Credential to access multiple AWS accounts (using cross-accounts), then in **Role Name** or **Role to Assume**, type just the AWS role name you've set up in AWS (no need to enter the entire ARN).

   If you are using cross-accounts, see "Authenticating to multiple AWS accounts using a single Amazon Credential" on page 942.

c. In cases where you need an External ID, you can type it here in the **External ID** field.

   ### About Amazon's External ID

   The primary function of *External ID* is to address and prevent the "confused deputy" issue. The External ID makes it less likely that a non-Trust Protection Platform user can access the other AWS account. Without the External ID protection, any IAM user within the AWS account where the Trust Protection Platform user resides, would be able to access the other AWS accounts simply by knowing the name of the role in the other account.

   When applying account credentials to provision a certificate, Amazon requires an External ID. The value must have a minimum of 2 characters and a maximum of 1,224 characters. The value must be alphanumeric without white spaces. It can also include the following symbols: plus (+), equal (=), comma (,), period (.), at (@), colon (:), forward slash (/), and hyphen (-).

   For more information, visit Amazon's article, How to Use an External ID When Granting Access to Your AWS Resources to a Third Party.

d. When you're finished, click **Save**.

7. (Conditional) If you selected **ADFS** from the **Source** drop-down list, then do the following:

   a. In the **ADFS Username Credential** field, select an Amazon credential.

      If you haven't yet created a user name credential for use with Amazon, click **Create New Credential** to define a new one, and then continue.

   b. In the **Web Service URL** field, type the full URL of your ADFS server.

   c. From the **Role** list, select the account that has the required permissions.

DID YOU KNOW? Each of the roles that appear in the Role list uses the following format:

arn:aws:iam::*AWSAccountNumber*:role/ *RoleMappedToADgroupByADFS*

So, for example:

arn:aws:iam::123423455678:role/MYCO-VenafiTPP

For more information about setting up your federated sign-in through Active Directory (AD) and ADFS, visit https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/.

d. When you're finished, click **Save**.

8. (Conditional) If you selected **EC2 Assigned Role** from the **Source** drop-down list, just click **Save** to finish.

   When you select this option, Trust Protection Platform authenticates with permissions that are assigned to the EC2 server on which it is running.

   IMPORTANT If you don't see this mode in the Source list, you don't have the proper permissions to use it. You must be either a master administrator, or you must request that you be added to the authorized identities list for using the AWS EC2 Assigned Role. To continue, contact a master administrator. See "Authorizing the use of EC2 Assigned Role for Amazon credentials" on page 941.

Creating Adaptable Credentials

Adaptable Credentials automate the retrieval of secrets from your third-party password vaults without compromising the security of your secrets.

The Adaptable Credential driver lets you create *username/password* and *password* credentials for retrieving their associated secrets that are stored by your third-party password vault. After creating your credentials, you assign them to certificates, applications and devices. During certificate enrollment and provisioning, their associated secrets are retrieved from the vault and are never stored in Trust Protection Platform.

Adaptable drivers depend on a Microsoft PowerShell script hosted in your local environment to execute functions corresponding to standard certificate lifecycle stages or Trust Protection Platform events. Typical of other adaptable drivers, you use a customized PowerShell script for each vault from which it can retrieve required details, including user names, paths, accounts names, etc. You specify which details to retrieve using the custom fields portion of the script.

To learn more about Venafi Adaptable Drivers and PowerShell scripts, see About Venafi Adaptable Driver PowerShell scripts in the *Administration Guide*.

First things first

Before you continue, consider the following prerequisite steps:

- Depending on your role in using Adaptable Credentials, you'll either need someone to provide you with a customized Adaptable Credential PowerShell script, or you'll need to create one.

  If your role is to create the script, then you can begin by using Template.ps1 (included in the *drive*:\Program Files\Venafi\Scripts\AdaptableCredential folder on your Trust Protection Platform server), or by downloading the HashiCorp Vault sample reference script from marketplace.venafi.com.

  To get started, see "PowerShell script reference for Adaptable Credential " on page 966.

  However you choose to create the script, it must be customized to your third-party password vault and placed in the correct folder of your Trust Protection Platform server before you can successfully create your new credentials.

- Make sure you have *View*, *Write*, and *Create* permissions to the folder where you plan to create your new credential object.

Getting started

With your customized Adaptable Credential PowerShell script placed in the /Venafi/Scripts folder on your Trust Protection Platform server, you're ready to set up your Adaptable Credential to automate the retrieval of secrets from your vault.

Complete the following tasks:

- "Step 1: Create an Adaptable Credential connector in VCC" below
- "Step 2: Create and configure an Adaptable Credential in Aperture" on the facing page
- "Step 3: Assign your new credentials to certificates, applications or devices" on page 924

Step 1: Create an Adaptable Credential connector in VCC

A *connector* is required if you want to connect Trust Protection Platform to your password vault. Connectors are configured in VCC and are essential for connecting Trust Protection Platform with third-party software and hardware.

When you create an Adaptable Credential connector, you'll select your PowerShell script and specify settings for connecting Trust Protection Platform with your third-party password vault.

> **TIP** The Adaptable Credential Connector is visible to all Venafi Trust Protection Platform servers that connect to the same database.

To create an Adaptable Credential Connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console** (VCC), and then open the **Connectors** node.
2. In the **Actions** panel, click **Create Adaptable Credential Connector**.
3. (Conditional) If requested, enter your Trust Protection Platform administration credentials.
4. In the **Create Adaptable Credential Connector**, do the following:
5. In **Connector Name**, type a unique and descriptive name for your new connector.
6. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
7. Under **PowerShell Script**, select your custom Adaptable Credential PowerShell script.
8. (Conditional) Under **Connection details**, type the service address and credential needed to connect to your access management platform.
9. (Optional) Under **Identities with access to this connector**, select those users and groups who should be allowed to create Adaptable Credentials using your connector.
10. (Conditional) If this is the first time you're creating an Adaptable Credential connector, then restart the Policy Tree application pool on all Trust Protection Platform web servers.

Step 2: Create and configure an Adaptable Credential in Aperture

With both your Adaptable Credential PowerShell script and connector in place, you can now use Aperture to create your Adaptable Credentials.

To create an Adaptable Credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **Adaptable Credential**.
3. Click **Folder** and select the policy folder in which to create your new credential.
4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.
1. In **Edit Credential Settings**, click **Credential Connector** and select the Adaptable Credential connector that you created previously.
2. Click the **Credential Type** list and select either **Password Credential** or **Username Password Credential**.
3. (Conditional) Complete all required custom fields related to your password vault.

   These fields are defined by your PowerShell script and should describe which secrets are to be retrieved from your password vault. If you did not write your script and have questions, contact the person who created the script for you.
4. (Optional) In **Description**, type a description of your new credential.

   A strong description can be useful in helping other administrators better understand the purpose of your new object (such as certificates, jobs, credentials, devices, trust stores, etc.), or to remind yourself later why you created it.
5. (Optional) Click **Contacts** and select one or more users or groups to whom you want default system notifications to be sent.

   The default contact is the master administrator.

   For more information about selecting contacts in Trust Protection Platform, see "Specifying who should get default system notifications" on page 697.
1. When you're finished, click **Save**.

Step 3: Assign your new credentials to certificates, applications or devices

By now, your Adaptable Credentials are ready to use. Because you can use your new credentials with several other types of objects in Trust Protection Platform, here are just a few ways you can use them in Trust Protection Platform:

- Authenticating to certificate authorities
- Setting the encryption password for private keys
- Setting the registration password for Server Agents
- Authentication to your Email server for Notifications
- How the SSH Protect product authenticates to SSH Servers for managing SSH Keysets agentlessly

About generic credential object configuration settings

The generic credential object stores a generic file paired with a password. This object is reserved for future use. For information about it's settings, see the table below.

Field	Description
Import	Allows you to import the generic file.
General	
Credential Name	Name for the generic credential object. This is a mandatory field.
Description	Description of the generic credential object.
Contact	User or group Identities assigned to this object.Default system notifications are sent to the contact identities. Default contact = master administrator **To select the object contacts** 1. Click the **Browse** button. The Identity Selector dialog opens.

Field	Description
	If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, you can enter the wildcard character (*). 2. Select a User or Group Identity, and then click **Select**. Press Shift+click to select multiple, contiguous users and groups. Press Ctrl+click to select multiple, discontiguous users and groups.
Settings	
Expires	Date when this credential expires. **IMPORTANT** The expiration date is used only to send a log notification. Trust Protection Platform continues to use the credential even if it is past its expiration date. **To set an expiration date** 1. Click the Selector button. The pop-up calendar displays. 2. Select a month and a year. 3. Click the day when the credential is to expire. The date displays in the text box (for example, 09/23/2017).
Credential	
Password/Confirm	Required to use the certificate.

Field	Description
Credential Stored	Indicates whether the generic file is stored (Yes/No).

General Tab

Permissions	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Creating credentials using Policy Tree

You can create all credential types from either the Credentials or Policy trees in Policy Tree. Several credential types can be created using Aperture. Aperture is the preferred method for creating credentials, but you can create credentials using Policy Tree. See "Creating new credentials " on page 912.

> **NOTE** To create new credential objects, you must have the View, Write, and Create permissions for the Credential or Policy tree where you plan to create them.

For more information about credentials, see "Working with system credentials" on page 909.

To create new credentials using Policy Tree

1. From the TLS Protect menu bar, click Policy Tree.
2. Select the **Credentials** or **Policy** tree from the Tree drop-down menu.
3. Do one of the following:
   - In the **Credentials** tree, select the Root Credential object, and then click **Add**.
   - In the **Policy** tree, select the Policy, Device, or Application object where you want to create the credential object, and then click **Add > Credentials**.
4. Click the credential object you want to create:

- Amazon AWS Credential

  For more information, see "About Amazon credentials" on page 940 in the *Administration Guide*.

- Adaptable Credential

  For more information, see "Creating Adaptable Credentials" on page 921 in the *Administration Guide*.

- Certificate Credential

  For more information, see "Creating certificate credentials" on page 918 in the *Administration Guide*.

- CyberArk Username Password Credential

  For more information, see "Using CyberArk with Trust Protection Platform" on page 944 in the *Administration Guide*.

- Generic Credential

  For more information, see "About generic credential object configuration settings" on page 925 in the *Administration Guide*.

- Google Credential

  For more information, see Creating a Google Credential in the *Certificate Authority and Hosting Platform Integration Guide*.

- Private Key Credential

  For more information, see "Creating private key credentials" on page 916 in the *Administration Guide*.

- User name or Password Credential

  For more information, see "Creating user name or password credentials" on page 913 in the *Administration Guide*.

5. Define the credential object configuration settings for the credential type you chose.
6. When finished, click **Save**.

Managing existing credentials

If you need to modify, move, or delete existing credentials, look no further than the Credentials inventory in TLS Protect (**Inventory** > **Credentials**).

One of the most common reasons to update credentials is when your organization's security policy requires you to change username and password credentials. And sometimes you just need to clean up by deleting credentials no longer in use.

From the Credentials inventory, you can view details about a specific credential, including where it's used and the permissions applied to it. You can move, rename, or delete a credential. And you can even replace the private key of a private key credential by simply dragging and dropping in a new one.

> **TIP** Each row in the Credentials inventory includes a *quick action button* that lets you apply actions on the credential, such as moving or deleting. For private key credentials, you can even replace its associated private key with another private key (see "Replacing a private key credential's private key" on page 938).

The Credentials inventory shows you the credentials stored in the system and lets you filter the list, making it easier to locate specific types of credentials.

What information is shown in the credentials Inventory?

The Credentials inventory displays a list of all or your credentials, along with columns of additional information about each credential. You can customize the inventory by adding, removing, and sorting columns.

Here are the available columns, which ones are visible by default, and which of them are sortable.

Column	Description	Default	Sortable
Name	The name of the credential given by the user when the credential was created.	Yes	Yes
Type	The type of credential. Trust Protection Platform has several types of credentials. The actual credential types you see depends on the products you have licensed. The credential types can include: ■ Adaptable Credential (*Username/Password*, and *Password*) ■ Amazon Credential ■ Certificate Credential ■ CyberArk Username Private Key Credential ■ Generic Credential ■ Google Cloud CA Credential ■ Password Credential ■ Private Key Credential ■ Username Password Credential	Yes	Yes
Folder	The folder location in the tree where the credential is stored.	Yes	Yes
Contacts	The list of contact(s) created by the user who created the credential.	No	No
Created On	The date the credential was created.	No	Yes
Description	The description provided by the user when they created the credential.	No	Yes

Can I see all existing system credentials in my Credential's inventory?

Your ability to see credentials in the system is limited by your permissions. If you have the *create* permission to the Policy root folder or if you have the *read* permission to at least one credential in Trust Protection Platform, then you can see the **Credentials** item in the **Inventory** menu. Otherwise, it won't be visible.

In addition, only those credentials to which you have the *read* permission are visible to you in Credentials inventory.

Filtering credentials in the credential inventory

You can expand the Credential Properties filter, and you can filter on any of the columns.

You can use filters to quickly find items in Venafi Platform inventories. Items that can be filtered include certificates, SSH keys, devices, identities, credentials, or Server Agents.

From any inventory list you can apply one or more filters to narrow the results. For example, use filters when you want to find a specific item, or find a group of items that meet a more specific set of criteria.

Filter Panel Types

The filter panel contains the following filters:

- **Credential Properties.** This is a list of properties that allows you to find credential objects based on specific properties related to the item.

To refine a list of discovered objects Using Filters

1. From the menu, open any of the inventory list views.

   For example, click **Inventory** > **Credentials**.

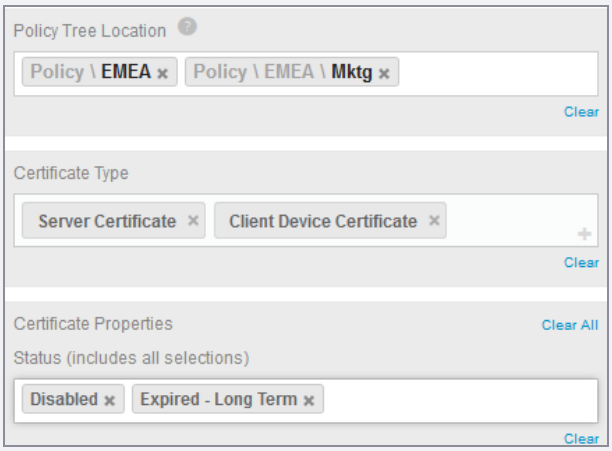
2. Using Filters, select and apply one or more filters to narrow the list of discovered items.

   > **DID YOU KNOW?** As you select and remove filters, the inventory list is automatically refreshed giving you instant filter results.

3. When you find the object you want in the inventory, click its name to view details.

EXAMPLE How search filtering works

All of the selections in a filter field are **OR** fields.



In the example above, the search could be described in the following way:

Show me all certificates with (policy location of EMEA or EMEA/Marketing) *and* (a certificate type of Server Certificate *or* a Client Device Certificate) *and* (Status of Disabled *and* Expired-Long Term).

List of Credential Properties filters

The following filters are available on the Credential Inventory page.

Common Filter	Description	Multi-value Support	Type
Name	Filters based on the credential name.	No	Partial match search (starts with)
Description	Filters based on the description of the credential	Yes / OR	Search from list
Contacts	Filters based on the credential's contact name or group. You can select multiple contacts, if needed.	Yes / OR	Search from list

Common Filter	Description	Multi-value Support	Type
Folder	Filters based on the certificate's parent folder. When you select at least one folder, a checkbox appears allowing you to search through all sub-folders as well.	Yes / OR	Select from list
Credential Type	Filters based on the type of the credential. E.g. Amazon Credential, Certificate Credential, CyberArk Username Password Credential, etc.	Yes / OR	Select from list
Created On	Date the credential was created. Can specify a specific date range, or a dynamic date range (next 60 days)	Date Range	Explicit or dynamic range

NOTE Companion public keys (`.pub` files) are stored in the database but are not displayed in the Trust Protection Platform web browser. However, these keys are still discoverable and will be rotated as needed.

Viewing information about a specific credential

You can click on any credential name to view the permissions screen that controls access to who can see the credential.

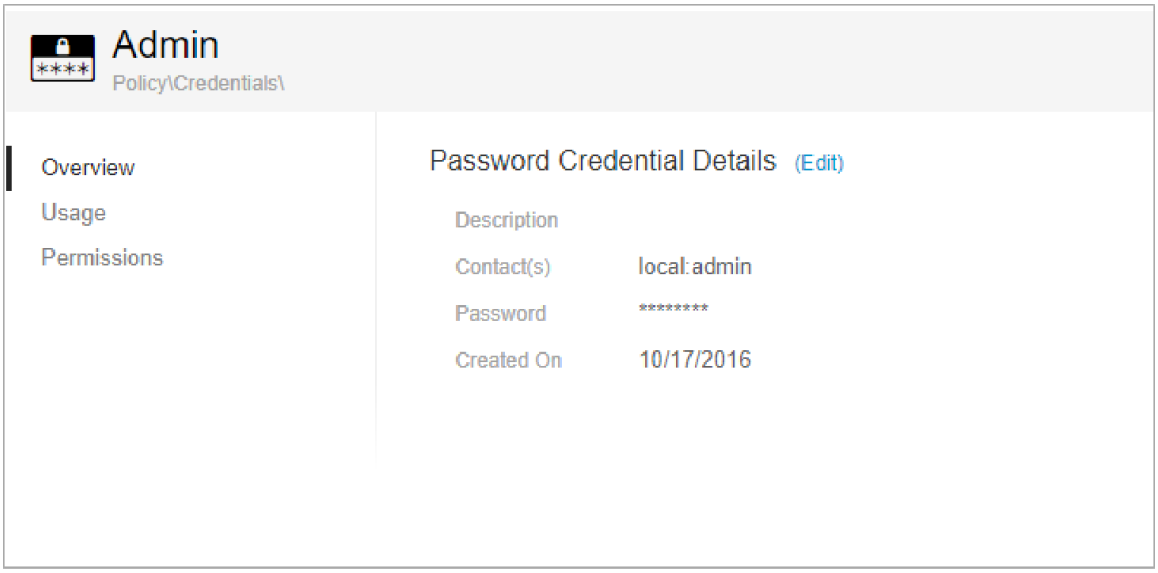
The credential details page shows you information about the credential, and allows you to take action on a credential. For more information, see "Exploring credential details" below.

Exploring credential details

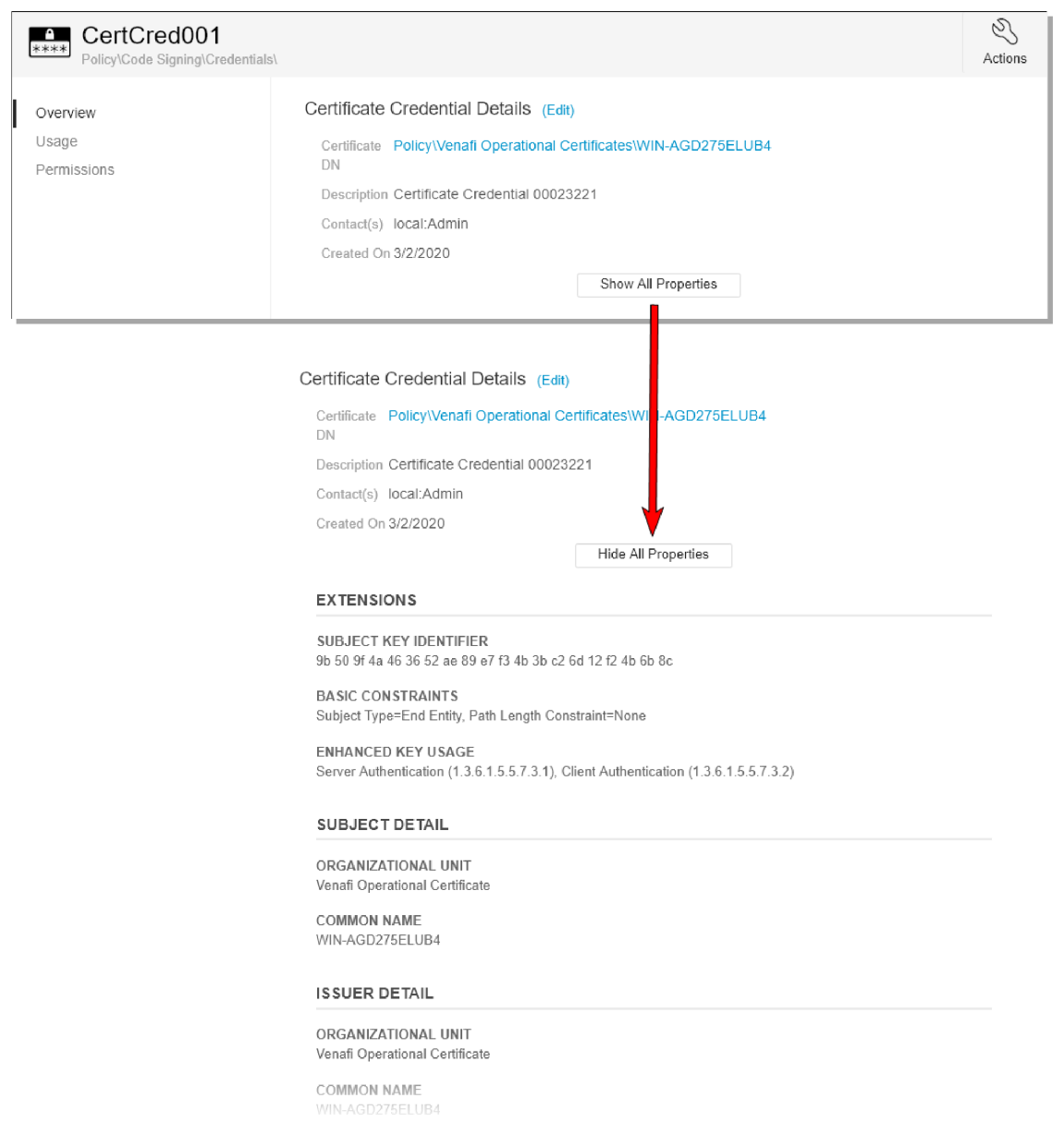
When you want to know how a credential is being used, or when you want to review its assigned permissions, you can view the credential's details from the Credential inventory (**Inventory** > **Credentials**). This information can help you better manage your credential objects and the items used by them, and can also help you with troubleshooting.

To learn about actions you can take on existing credentials, see "Editing credentials" on page 937.

The details view of a credential shows you information about the credential, including the folder where the credential object exists, items that are using the credential (devices, CAs, etc.), and the local and cumulative permissions set on it.

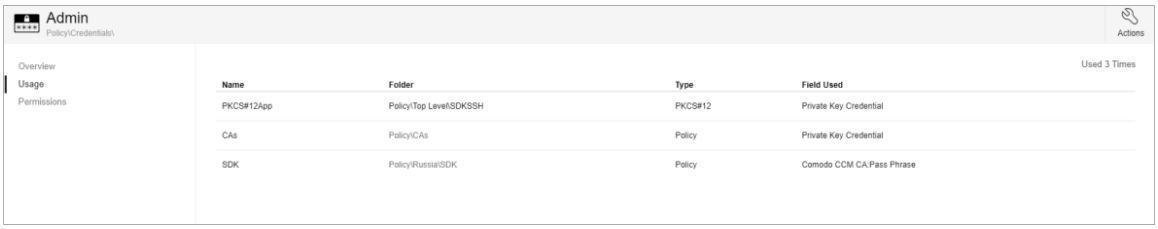


DID YOU KNOW? Because *certificate credentials* are linked to a specific certificate, you can click the **Show All Properties** button to see all the certificate's properties.



Viewing how a credential is being used

If you want to know what other objects in Trust Protection Platform depend on a specific credential, go to the **Usage** panel on a credential's details page. Knowing how a credential is getting used can help you to make better decisions when updating, moving, or deleting credentials. It's also helpful while troubleshooting.



The Usage panel includes the following data points that can give you a clearer picture of how other objects are referencing a credential:

Field	Description
Name	The name of the device or installation that is using the credential, or the name of the CA template using the credential.
Folder	The location or device where the credential is used.
Type	The type of item using the credential, such as a device, an installation, a CA template, etc.
Field Used	What field on the item is actually using the credential. Some items have multiple places where credentials are set, so this shows you which field uses this specific credential.

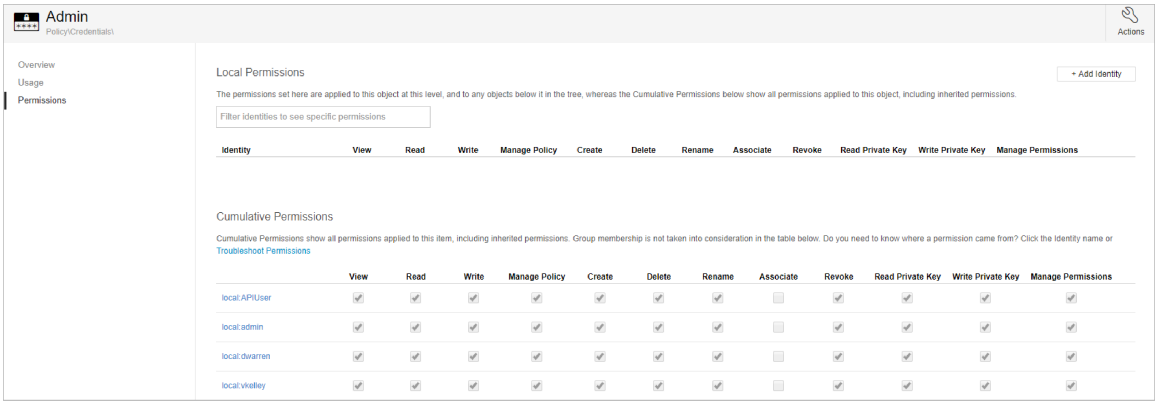
TIP Only the first 100 usages of a credential are shown. If the credential is used in more than 100 locations, a message appears that will tell you that there are more, but that you cannot load or view them.

IMPORTANT The Usage panel only shows attributes that are set directly on an item or folder. Policy values that are in effect are *not* taken into consideration.

For example, if a device has a credential set via policy, the table shows the folder where the policy is set, not a list of all the devices that the credential applies to. If the credential was also set on one of the devices in the list, then the table would show both the folder where the credential is applied, as well as the device that has the (redundant) credential applied.

Exploring permissions assigned to a credential

Permissions for credentials function in the same way they do for other objects in Trust Protection Platform. The Permissions panel in a credential's details page show you the level of permissions currently applied directly to the object (Local Permissions) and those that are applied through inheritance (Cumulative Permissions).



For information about working with permissions, see "About permissions" on page 721 and "Assigning permissions to objects" on page 730.

Editing credentials

After creating credentials, you'll likely need to edit, move, or even delete them. You can perform these functions from the Credential inventory (**Inventory** > **Credentials**).

About editing user name or password credentials

When editing a user name or password credential, if you don't want to change the password, leave the field blank, and edit the other fields. The password will not be changed.

DID YOU KNOW? When editing a user name or password credential, the password fields show dots to indicate that there is a password set in the secret store. This password is not actually retrieved from the secret store when you are editing the credential settings, and the existing password is not compared to the value of the password field. If TLS Protect detects a change to the password field, TLS Protect will update the password in the secret store with the new value. If the password fields are not modified, nothing happens to the password in the secret store.

To edit a credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials** to open the Credential inventory list.
2. Locate the credential you want to edit.

   You can use filters, if necessary.

   See "Managing existing credentials" on page 929.
3. Click the **Edit** quick action button at the right end of the row that contains the credential you want to edit.

   If you're already in the details view of a credential, click the **Edit** link to the right of the credential's title.
4. In **Edit Credential Settings**, make your changes, and then click **Save**.

   For specific details related to the type of credential you're editing, refer to the related topic:

   - "Creating user name or password credentials" on page 913
   - "Creating private key credentials" on page 916
   - "Creating certificate credentials" on page 918
   - "About generic credential object configuration settings" on page 925

Replacing a private key credential's private key

If you need to change the private key used in an existing private key credential, you can do so from the Credential inventory (**Inventory** > **Credentials**).

If you're looking for steps to create a new private key credential, see "Creating private key credentials" on page 916.

To replace a private key credential's private key

1. From the TLS Protect menu bar, click **Inventory** > **Credentials** to open the Credential inventory.
2. [(Optional) Use the filters to show only Private Key credentials, then use other filters as necessary to help you locate the credential you want to change.
3. Click **Change Private Key** on the quick action button.
4. In the **Import Private Key** box, do **one** of the following:
   - Locate the new private key on your local computer, then drag it into the **Import Private Key** box.
   - Click inside the upload box in the **Import Private Key** window, browse to the location of the new private key on your local computer, and then click **Open**.
   - Click **Paste the private key text**, and then copy and paste the entire contents of the private key file.
5. Click **Upload**.

Moving a credential to another folder

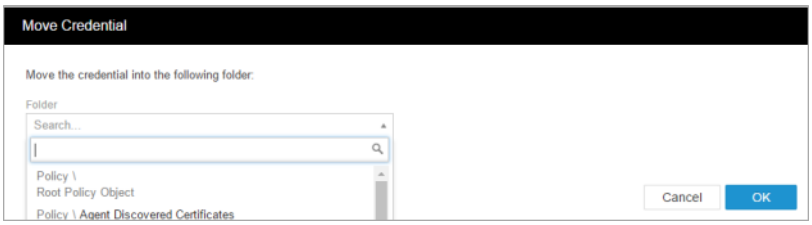
If you simply want to move an existing credential to another folder, you can use the Move quick action button in the Credentials inventory (**Inventory** > **Credentials**).

> **TIP** Keep in mind that if the folder where you want to move an existing credential already contains an item with the same name, Trust Protection Platform won't let you move the credential to that folder. In that case, simply rename either one of the two credentials before you make the move.

To move a credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials** to open the credential inventory list.
2. Locate the credential you want to edit.

   You can use filters, if necessary.
3. Click the **Move** quick action button.
4. Use the **Folder** search box to select the folder locaton where you want to store the credential.



5. Click **OK**.

Deleting credentials

You can delete existing credentials from the Credential inventory (**Inventory** > **Credentials**). But before you delete a credential, make sure you know if other objects depend on it. For more information, see "Viewing how a credential is being used" on page 936.

> **DID YOU KNOW?** Trust Protection Platform won't actually let you delete a credential that is currently linked to one or more objects. If you try to delete a linked credential, Aperture displays a list of linked objects. In that case, you'll need to remove the credential link from the other objects before you can delete the credential.

To delete a credential

1. From the TLS Protect menu bar, click **Inventory** > **Credentials** to open the credential inventory list.
2. Locate the credential.

   You can use filters, if necessary.
3. Click the **Delete** quick action button.

   You will see a confirmation window to verify that you really want to delete the credential.
4. Click **Yes, Delete** to delete the credential permanently from the system.

About Amazon credentials

You can create and use Amazon credentials with AWS services that are supported natively by Trust Protection Platform. See Supported integrations with Trust Protection Platform.

You create Amazon credentials in the same way you create other credentials in Trust Protection Platform. But the Amazon Credential offers three options for the source of your Amazon credential: *Local*, *Active Directory Federated Services* (ADFS), and *EC2 Assigned Role*.

- *Local* stores your password credentials in Trust Protection Platform.
- *ADFS* uses Active Directory credentials to authenticate with AWS using ADFS (SAML 2.0).
- *EC2 Assigned Role* (added in Trust Protection Platform version 20.4) is for use with instances of Trust Protection Platform that are running in EC2. You can use this role to acquire temporary access keys for issuing certificates from AWS, provisioning them, and for Onboard Discovery.

  > **NOTE** As an added security measure, you must be a master administrator or have been added to *AWS EC2 Role Authorized Identities* by a master administrator to use the EC2 Assigned Role mode. Without this security control, any user would be able to use this mode without the ability of administrators to verify it. Master administrators can add non-master administrator user accounts, as well as groups in Policy Tree (**Platforms** tree > **Platforms** > **AWS EC2 Role Authorized Identities** tab).

For common questions and answers about Amazon credentials, see FAQ: Amazon Credentials.

Authorizing the use of EC2 Assigned Role for Amazon credentials

EC2 Assigned Role (added in Trust Protection Platform 20.4) is for use with instances of Trust Protection Platform that are running in EC2. You can use this role to acquire temporary access keys for issuing certificates from AWS, provisioning them, as well as for Onboard Discovery.

As an added security measure, you must either be a master administrator or have been added to *AWS EC2 Role Authorized Identities* by a master administrator to use EC2 Assigned Role as the source for your Amazon credential. Without this security control, any user would be able to use this mode without the ability to verify that they're entitled to use it.

> **NOTE** The following procedure is for master administrators. If you're not a master administrator, contact one and request that you be added to the EC2 Assigned Role Authorized Identities list. Consider sharing the URL of this page with your administrator if she's not familiar with this feature.

To authorize users or groups to use the EC2 Assigned Role option

1. From the TLS Protect menu bar, click **Policy Tree**.

2. Select the root platforms object and this click the AWS EC2 Role Authorized Identities tab.
3. Click  and move identities from **Available** to **Selected**, and then click **Select**.
4. When you're finished adding identities, click **Save**.

Authenticating to multiple AWS accounts using a single Amazon Credential

If you have multiple AWS accounts–such as production accounts and testing or QA accounts–you can configure Trust Protection Platform to authenticate to multiple AWS accounts at once. This configuration lets you authenticate to a single AWS account and execute different types of work–provisioning, and Onboard Discovery–across any other AWS accounts in which you've added the same cross-account role.

You can configure an Amazon credential object in Trust Protection Platform with a single set of AWS access keys (ID and Secret), specifying an Amazon *cross-account IAM role* (defined in one of your AWS accounts) and an External ID (if one is used).

About Amazon's External ID

The primary function of *External ID* is to address and prevent the "confused deputy" issue. The External ID makes it less likely that a non-Trust Protection Platform user can access the other AWS account. Without the External ID protection, any IAM user within the AWS account where the Trust Protection Platform user resides, would be able to access the other AWS accounts simply by knowing the name of the role in the other account.

When applying account credentials to provision a certificate, Amazon requires an External ID. The value must have a minimum of 2 characters and a maximum of 1,224 characters. The value must be alphanumeric without white spaces. It can also include the following symbols: plus (+), equal (=), comma (,), period (.), at (@), colon (:), forward slash (/), and hyphen (-).

For more information, visit Amazon's article, How to Use an External ID When Granting Access to Your AWS Resources to a Third Party.

DID YOU KNOW? Like most Trust Protection Platform applications, AWS makes use of the Hostname/Address setting from its parent device object, even though it's a cloud service and not a typical device. This is because AWS is an Internet-based service with a public interface that is the same for all customers. But if you're provisioning to a secondary account, the parent device's Hostname/Address setting in Trust Protection Platform is actually used to specify the AWS account ID (rather than the expected hostname or address).

This is a confusing but temporary method for managing this specific use case.

For more information about AWS configuration, see Amazon Web Services (AWS)—Overview.

For the ADFS Amazon credential, no additional setup steps are required. This is because ADFS is already tied to a specific account and role. So on the credential, you don't specify the account information.

NOTE The following procedure is a high-level overview of the steps you need to take in both AWS and Trust Protection Platform. However, you should refer to your AWS documentation for details related to the AWS-specific steps in the following procedure.

TIP Consider reviewing the Amazon tutorial found at https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html.

To configure authentication to multiple AWS accounts using a single Amazon Credential

1. In a secondary AWS account—as apposed to your primary account where your Trust Protection Platform/Amazon Credential resides—do the following:
   a. Create a policy with the permissions outlined in AWS permission requirements.
   b. Create a role that gives access to your primary AWS account.
2. In your AWS primary account, do the following:
   a. Create an AWS policy that allows a user in the primary account to execute the AssumeRole operation in each of the secondary accounts.
   b. Grant the user referenced by the Trust Protection Platform's Amazon Credential the role from step 2a.
3. In Trust Protection Platform, create an Amazon Credential and specify the Access Key ID, Secret Access Key, and cross-account role of the AWS account (from Step 1b where you created the new role).

   For configuration details, see "About Amazon credentials" on page 940.

Using CyberArk with Trust Protection Platform

CyberArk Enterprise Password Vault, a component of the CyberArk Privileged Account Security Solution, is designed to discover, secure, rotate and control access to privileged account passwords used to access systems throughout the enterprise IT environment.

DID YOU KNOW? CyberArk is somewhat like a personal password management system: you store various passwords from multiple applications or services in a credentials vault and use a single *master password* to unlock the vault and gain access to an application or service.

If you're using CyberArk Enterprise Password Vault to manage credentials and you want to add privileged account credentials used by Venafi Trust Protection Platform, you can integrate CyberArk with Venafi and thereby eliminate the need to manage those credentials in both places.

For more about CyberArk Enterprise Password Vault, visit https://www.cyberark.com.

NOTE For information about supported versions of CyberArk Privileged Account Security for integration with Trust Protection Platform, see Supported integrations: devices, applications and services you can use with Trust Protection Platform in the *Certificate Authority and Hosting Platform Integration Guide*.

Getting CyberArk ready for integration with Trust Protection Platform

Implementing CyberArk with Trust Protection Platform (TPP) involves detailed setup on both platforms. The following information clarifies the tasks and platform responsibilities to speed up the process. Once set up correctly, the benefits clearly justify the initial effort.

CyberArk objects	Related CyberArk permissions for each CyberArk object	TPP objects	Action in Trust Protection Platform
Vault and Safe			
End User This is a user created in CyberArk that is used by TPP users who need an application or server to authenticate with CyberArk.	*Use accounts* or *Retrieve accounts* **NOTE** User may be granted access individually or via group membership. Access may not be granted using Object Level Access Control (OLAC). A reason cannot be required for the effective Master Policy to access the password for an account.		You must provide CyberArk credentials that have access to the safe whenever you create a CyberArk Username Password credential.
Application	*Retrieve accounts*		For Trust Protection Platform to use when it retrieves account passwords from a safe
Authorization User	*View Safe Members*		For Trust Protection Platform to verify that the Actual User is authorized to create CyberArk Username Password credentials
Providers	*Retrieve accounts*, *List accounts*, and *View Safe Members*.		Access required by the Application Identity Manager (AIM) installed on each Trust Protection Platform server

NOTE Refer to CyberArk Enterprise Password Vault documentation for help with tasks that must be completed on the CyberArk platform.

TIP Keep in mind that in CyberArk, "account" is analogous to "credential" in Trust Protection Platform. Terminology can be confusing as many security companies adopt their own nomenclature.

Step-by-step

Step	Platform	Task
1	CyberArk	Create a CyberArk vault and safe.
2	CyberArk	Create a CyberArk (PVWA) user for verifying a Trust Protection Platform user has access to a safe.
3	CyberArk	Grant access to CyberArk Application Identity Manager. Follow the steps when using either AIM/AAM or Central Credential Provider to grant access.
4	CyberArk	Create a CyberArk Application for Trust Protection Platform to use when retrieving accounts from safes. When using Central Credential Provider method also create an AIM Web Service application. **BEST PRACTICE** "About securing a CyberArk application " on page 948
5	CyberArk	Create a CyberArk end user (if one does not already exist). The credentials for this new CyberArk user will be used later when you create a *CyberArk Username Password Credential* in Trust Protection Platform. See "Adding and configuring CyberArk credentials" on page 958. Grant user either *Use Accounts* or *Retrieve Accounts* access to the safe.
6	Trust Protection Platform	If the password retrieval method will be through an AIM/AAM Agent, install the CyberArk Application Identity Manager (AIM/AAM) on all Trust Protection Platform servers. Installation is optional for servers which will never provision certificates using CyberArk credentials and are not hosting the web console. ■ Retrieve Accounts

		■ List Accounts ■ View Safe Members Grant all providers created by installing AIM/AAM (from Step 6) *Retrieve Accounts*, *List Accounts*, and *View Safe Members* access to the safe.
7	Trust Protection Platform	**NOTE** This step does not apply when using Central Credential Provider Configure the CyberArk connector in Venafi Configuration Console to connect to CyberArk using the web service (PVWA) user credential (from Step 2). See "Creating a CyberArk connector" on page 951. On the CyberArk Connector, configure the connection between Trust Protection Platform and the CyberArk service and configure all other settings as appropriate. For example, if you want the proxy to manage the CyberArk connection, be sure to enable the proxy settings. See "Configuring and editing the CyberArk Credentials driver in the Policy Tree" on page 956.
8	CyberArk	Grant the verification user–the PVWA user from Step 3–*View Safe Members* access to the safe. Grant the Application (from Step 4) *Retrieve Accounts* access to the safe.
9	CyberArk	Grant user (from step 5) either *Use Accounts* or *Retrieve Accounts* access to the safe. **NOTE** See Configuring and editing the CyberArk Credentials driver in the Policy Tree.
10	CyberArk	Create and set up a CyberArk Enterprise Password Vault account that will be used to manage the password of the credential for accessing the device.
11	Trust Protection Platform	Assign the CyberArk Password credential to applications and devices for provisioning. See "Using a CyberArk credential for provisioning (certificate installation)" on page 964

About securing a CyberArk application

Examples of settings that help ensure that only Trust Protection Platform can use the CyberArk application

- OS User for Trust Protection Platform:
  - NT AUTHORITY\SYSTEM (or a domain user account if TPP is using MSSQL with Windows Authentication)
- Path examples for Trust Protection Platform:
  - C:/Program Files/Venafi/Drivers/Credentials/CRCyberArkCredentials.dll
  - C:/Windows/Microsoft.NET/Framework64/v4.0.30319/mscorlib.dll (For version 12, with the correct .NET framework path that Trust Protection Platform uses because the assembly that communicates with version 12 loads dynamically.)
- Hash:
  - 0AA1E6B81A2097816B2A412B9FF4705FEB682DF1 (Generated by NetAIMGetAppInfo utility)

IMPORTANT You need to run the following on each of your Trust Protection Platform servers if you want to apply security using the Hash: "C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Utils\NETAIMGetAppInfo.exe" GetHash /AppExecutablesPattern "C:\Program Files\Venafi\Drivers\Credentials\CRCyberArkCredentials.dll

- Host:
  - Host IP address or Hostname or FQDN

See the *Application Authentication Methods* section of **CyberArk's Credential Provider and ASCP Implementation Guide** for details on how to apply these values.

Creating a CyberArk Application for TPP

Before following these steps, verify that CyberArk Vault, CyberArk PVWA, CyberArk SCIM Server (if available) and either CyberArk Central Credential Provider or Windows AIM/AAM Agent are installed and configured.

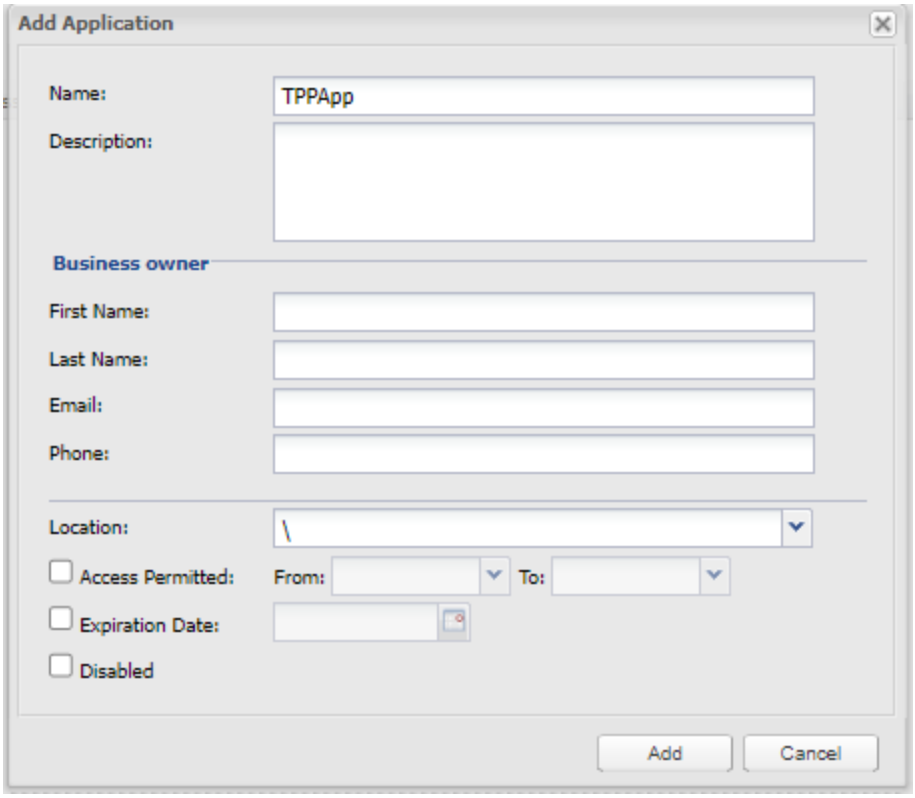
You will need the following information and access:

- FQDN of the CyberArk PVWA instance
- RDP access to the TPP engine

- Trust Protection Platform administrator with permissions to create credentials in Venafi Configuration Console

Configuring the CyberArk Credential Provider requires creating one or more applications in the CyberArk PVWA interface

1. Log in to the CyberArk PVWA interface, and select **Applications** > **Add Application**.
2. Provide a name for the application, for example **TPPApp**. This application will be used to authenticate the TPP server against CyberArk PVWA.

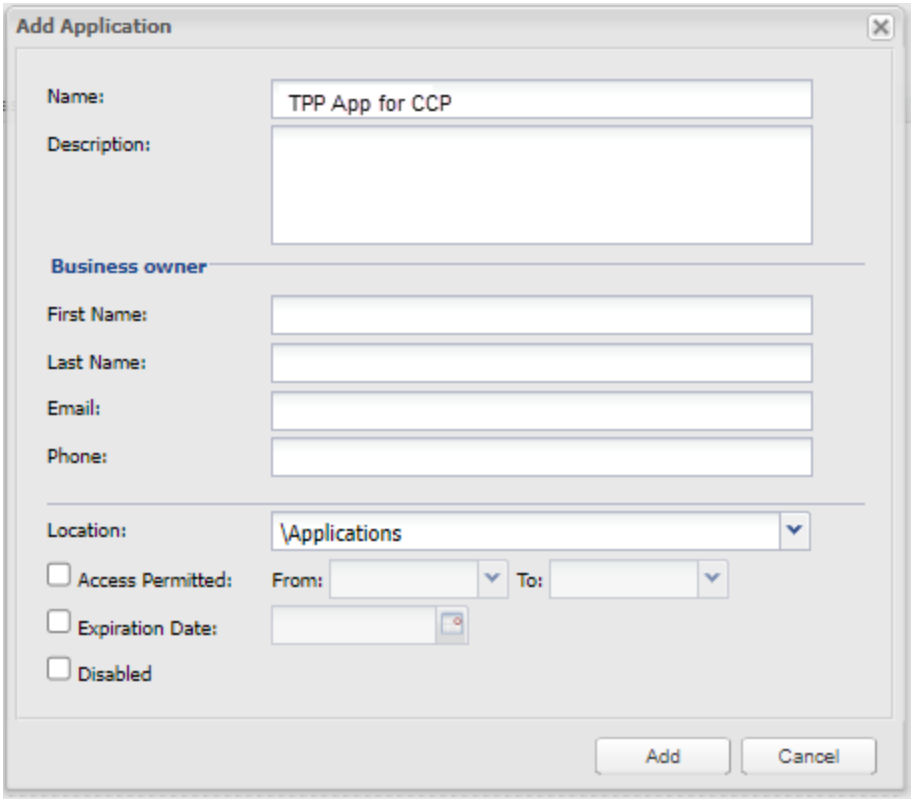


NOTE: This application will need to be a member of the Safe from which you want to retrieve the account (secret).

3. Click **Add**.

Complete the following steps only if Central Credential Provider is used to retrieve secrets

1. Select **Applications** > **Add Application**.
2. In the **Name** field enter **TPP App for CCP**.
3. Using the **Location** drop-down, select \Applications.



4. Click **Add**.
5. Add the credential provider of the AIM/AAM as a Safe Member.

   For example: Prov_<hostname of the machine where AIM/AAM is installed>.

   These provider objects MUST have these permissions to the CyberArk Safe:

   - Service Account: Select **View Safe Members** permission and access to the PVWA interface
   - End user account: Select **Retrieve accounts**
   - Application ID (for TPPApp): Select **Retrieve accounts**

- Windows AIM/AAM Agent credential provider (Prov_<hostname> one): Select **Retrieve accounts**, **List accounts** and **View Safe Members**

6. Click **Save**.

Creating a CyberArk connector

A connector is required if you want to connect Trust Protection Platform to a CyberArk Enterprise Vault. For detailed information on CyberArk, including prerequisites for configuration, see "Using CyberArk with Trust Protection Platform" on page 944.

> Before you continue, set up CyberArk correctly. See "Getting CyberArk ready for integration with Trust Protection Platform" on page 944.

The CyberArk connector works with all Venafi Trust Protection Platform servers that connect to the same database.

To create a CyberArk connector

1. On the Venafi Trust Protection Platform server, open the **Venafi Configuration Console** and open the **Connectors** node.
2. In the **Actions** panel, click **Create CyberArk Connector**.
3. (Conditional) If requested, enter your Venafi Trust Protection Platform administration credentials.
4. In the **Create CyberArk Connector** window, complete the following fields:

Field	Description
Connector Name	Provide a name for the connector.
Description	Type any additional information that describes this connection. For example, the description could include the name of the server where the CyberArk Application Identity Manager (AIM) is installed.
Use Trust Protection Platform permissions model for credential access management	Select this option to skip all verification checks against the CyberArk PVWA and SCIM services. Identities with View access to the Connector object are allowed to manage CyberArk credential objects. If this option is not selected, user validation is done via CyberArk PVWA.
Privileged Account Security Web Services URI	Enter the location of your CyberArk Password Vault Web Access (PVWA) endpoint. For example: `https://webservices.host.com:1234/PasswordVault/WebServices` or `https://example.privilegecloud.cyberark.com/PasswordVault/`
Use Proxy	Check the Use Proxy box if you want the proxy to manage the CyberArk connection. This setting applies to the interaction between Trust Protection Platform, CyberArk Password Vault Web Access (PVWA), and Central Credential Provider. The Application Identity Manager (AIM/AAM), which is a standalone software component, requires additional Vault.ini configuration as detailed in the CyberArk Application Identity Manager Implementation Guide.
Web Service User	Type the user name you created for Trust Protection Platform to use when verifying the permissions a user has been granted to a CyberArk safe. **NOTE:** This is not applicable when Certificate (PKI) authentication method is selected for the Web Services Authentication Method

Field	Description
	NOTE: This is a service account. The account must have View safe members permission to all safes that the end users are allowed to retrieve secrets. Refer to Check permissions on safe members for more details.
Web Service Password	Type the password for the user you created for Trust Protection Platform to use to verify CyberArk safe permissions. **NOTE:** This is not applicable when Certificate (PKI) authentication method is selected for the Web Services Authentication Method
Service Account Authentication Method	Select the authentication method to use to authenticate to the vault. Supported methods include CyberArk (1st gen API), CyberArk (2nd gen API), LDAP (2nd gen), RADIUS (2nd gen), Windows (2nd gen), and Certificate (PKI). **NOTE:** When Certificate (PKI) authentication method is selected, you MUST specify the certificate credential in **WebAdmin** > **Credentials tree** > **Credential Drivers** > **CyberArk Connector** .
SCIM Server URI (optional)	If you have a configured CyberArk SCIM server, add the SCIM service address. For example: https://scimserver.example.com/CyberArk/scim/v2 The main scenario for which TPP uses the CyberArk SCIM is when the end user (CyberArk, LDAP, RADIUS or Windows) that is retrieving the account (secret) is not a direct member of a Safe but is a member of a CyberArk group. In this case SCIM Server URI, SCIM Server User and SCIM Server Password MUST be provided on the

Field	Description
	CyberArk connector of TPP (see the TPP setup for CyberArk when retrieving accounts section). The group itself MUST be a member of the Safe and MUST have **Retrieve accounts** or **Use accounts** permission to the Safe for the end user to successfully retrieve the account (secret) from the Safe.
SCIM Server User SCIM Server Password	Enter the SCIM server URI, user name and password so that Trust Protection Platform can authenticate to your SCIM server. This is a service account created by the CyberArk administrator for use by TPP. This user MUST be able to authenticate to the CyberArk SCIM server Following successful authentication, your CyberArk connector setup is complete. **DID YOU KNOW?** If you specify the correct URL, user name and password and authentication fails, then Trust Protection Platform attempts to authenticate with the CyberArk user name and password.
Password Retrieval Method	Select a method to use for password retrieval. ◦ If you select **Windows Credential Provider (AAM Agent)**, then select a version from **Windows Credential Provider Version**. ◦ If you select **Central Credential Provider**, then enter the **Central Credential Provider Web Service URL**. If you use Central Credential Provider, then you don't need to install the CyberArk AIM/AAM agent on a Trust Protection Platform server. To configure certificate-based authentication to

Field	Description
	Central Credential Provider see Configuring and editing the CyberArk Credentials driver in the Policy Tree **DID YOU KNOW?** You can find the installed version of the Windows AIM/AAM Agent using RDP to the machine where the AIM/AAM agent is installed. Then open **Programs and features** and search for the CyberArk AIM/AAM Agent installation in the list and check its version.
Windows Credential Provider Version	This option is only available when Windows Credential Provider (AIM/AAM Agent) is selected. Select the version of the Windows AIM/AAM agent. **DID YOU KNOW?** You can find the installed version of the Windows AIM/AAM Agent through RDP to the machine where the AIM/AAM Agent is installed. Then open **Programs and features**, and search for the CyberArk AIM/AAM Agent installation in the list to check its version.

5. Click **Create**.
6. Restart IIS.

You can see the new connector in the **Credential Connectors** section of the Venafi Configuration Console. You will also be able to see the connector, as well as the new server user credential that was created, in Policy Tree, in the Credentials tree.

NOTE Trust Protection Platform only supports one CyberArk connector. You cannot connect to multiple CyberArk vaults.

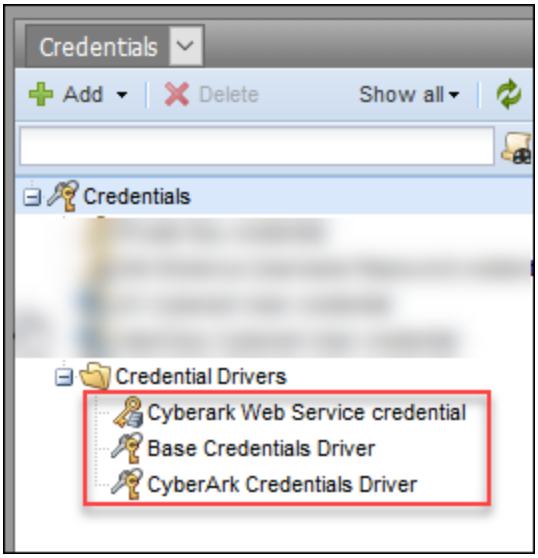
Configuring and editing the CyberArk Credentials driver in the Policy Tree

After you create a CyberArk connector in Venafi Configuration Console (VCC), the connector appears in the Credentials tree.

You can also configure a SCIM server for cases where a CyberArk user is granted access to a CyberArk safe through a group rather than being granted access to their user account directly.

To edit the configuration of a CyberArk credential in Policy Tree

1. Open the **Policy Tree** and go to the **Credentials** tree.
2. Open the CyberArk credentials driver (the name you see depends on the name you gave the connector in VCC).



3. Add or edit the **Description** and specify the **Contact(s)** for this driver.
4. (Optional) Select **Disabled** if you want to turn off CyberArk functionality.
5. (Optional) Select **Use Proxy Settings** if you want the proxy to manage the CyberArk connection.

> **NOTE** This setting only applies to interactions between the Trust Protection Platform server and CyberArk Password Vault Web Access (PVWA). The Application Identity Manager (AIM/AAM), which is a standalone software component, requires additional Vault.ini configuration as detailed in the *CyberArk Application Identity Manager Implementation Guide*.

6. (Optional) Select **Use Trust Protection Platform permissions for credential access management** to skip all verification checks against the CyberArk PVWA and SCIM services. Identities with View access to the Connector object are allowed to manage CyberArk credential objects. If this option is not selected, user validation is done via CyberArk PVWA.

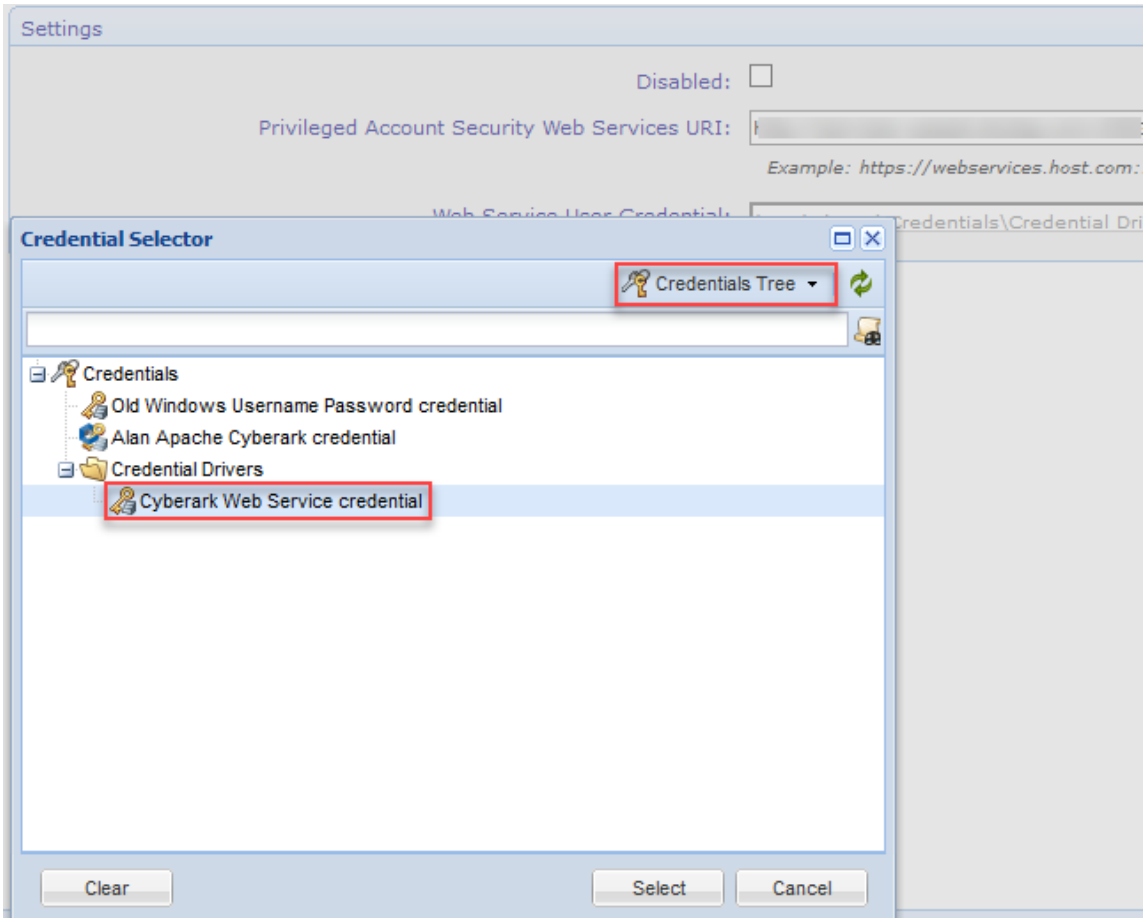
7. In **Privileged Account Security Web Service URI**, enter the location of your Components server.

   Refer to CyberArk's documentation for more information.

8. From the **Service Account Authentication Method** drop-down list select the authentication method to use to authenticate to the vault.

9. For **Service Account Credential**, click ..., then select the CyberArk web service credential (PVWA) that contains the web service user name and password.

   For more information, see "Editing the CyberArk Web Service credential" on page 959.



10. From the **End User Authentication Method** drop-down list select the authentication method to verify that the user authenticated to the Trust Protection Platform has permission to retrieve the account secrets.

11. Select a **Password Retrieval Method**.
    - If you select **Windows Credential Provider (AAM Agent)**, then select a version from **Windows Credential Provider Version**.
    - If you select **Central Credential Provider**, then enter the **Central Credential Provider Web Service URL**. Entering the URL for password retrieval through a Central Credential Provider web service eliminates the need to install the CyberArk AIM/AAM agent on a Trust Protection Platform server.
    - If you select **Central Credential Provider**, select the **Certificate Credential**. This credential is used when Central Credential Provider has certificate-based authentication configured.

12. (Optional) If you are using a SCIM server for cases where a CyberArk user is granted access to a CyberArk safe through a group rather than being granted access to their user account directly, do the following:
    a. In **SCIM Server URI**, enter the location of your SCIM server.
    b. In **Service Account Credential**, click ..., then select the SCIM credential.

13. Click **Save**.

Adding and configuring CyberArk credentials

You can create CyberArk credentials and assign them to certificates, applications, and devices during the provisioning process. Trust Protection Platform is able to retrieve credentials stored in your CyberArk Enterprise Password Vault.

> **IMPORTANT** To see the permissions you need to perform this task, see "CyberArk user and password integration requirements" on page 963.

To create CyberArk credentials

1. From the TLS Protect menu bar, click **Inventory** > **Credentials**, and then click **Create a New Credential**.
2. Click the **Credential Type** list and select **CyberArk Username Password** or **CyberArk Password**.
3. Click **Folder** and select the policy folder in which to create your new credential.

4. In **Credential Name**, type a unique name for the new credential object, and then click **Create and Configure**.

5. (Conditional) If you selected the **CyberArk Username Password** credential type (in Step 2), then in the **User Name** field, type the user name that Trust Protection Platform will use when provisioning a certificate to a device.

   This should match the User Name property of the account you created in the CyberArk safe.

6. In **Application ID**, type the name of the CyberArk user that you created for the Application Identity Manager installed on your Trust Protection Platform servers to use when retrieving a password from CyberArk. Refer to Check CyberArk permissions on safe members for details.

7. Complete the remaining fields:
   a. **Safe Name**: from the CyberArk Vault.

   b. **Folder Name**: from the CyberArk Safe.

      > **NOTE:** If no folder was used during the creation of the account (secret) in CyberArk, enter Root.

   c. **Account Name**: from the CyberArk Safe.

   d. **CyberArk Username**: This is the end user account (not the service account configured in VCC). It is needed ONLY to verify that the user authenticated to Venafi TPP has permission to retrieve the account (secret) specified above thus, to create credential in TPP. The required permission for this user in CyberArk is Retrieve accounts or Use accounts.

   e. **CyberArk Password**: The password for the end user account

8. When you have completed the required fields, click **Save**.

> **IMPORTANT:** The credential object will be saved ONLY in case of successful retrieval of the account (secret) from the CyberArk Vault. If the credential object was not saved for some reason, you can refer to section “Common Error Messages”.

Editing the CyberArk Web Service credential

After you've set up user credentials in CyberArk, you'll need to set up and configure the same user credentials in Trust Protection Platform.

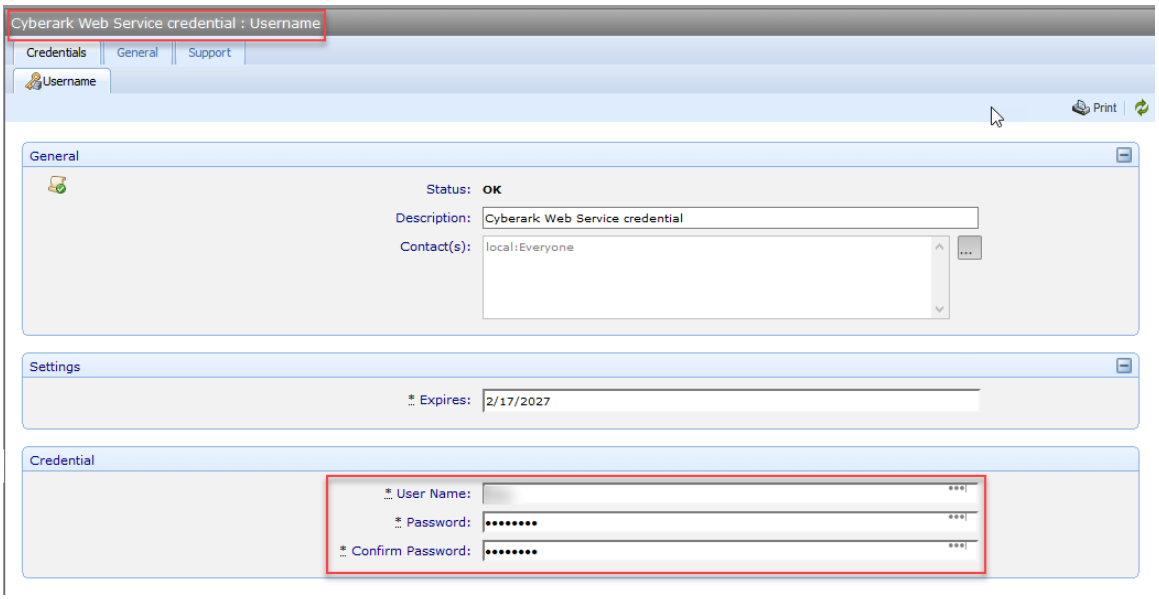
The username credential is created automatically by the Venafi Configuration Console when you create the CyberArk connector. If you need to edit the credential you can either modify the connector in Venafi Configuration Console, or you can edit the username credential in the Policy Tree.

To edit the CyberArk username credential in the Policy Tree

1. In the Credentials tree, locate the CyberArk username credential you want to edit.
2. In the **Description** field, enter a meaningful description.

   The description should reflect that it is a CyberArk Web Service credential.
3. Set an expiration date. Note, however, that the CyberArk vault settings may take precedence if expiration set there is earlier.
4. In the **Credential** field, specify the *same* User Name and Password that you set up in the CyberArk vault.

   IMPORTANT The credential must be exactly the same or Trust Protection Platform will not be able to communicate with CyberArk.



5. Click **Save**.

Granting access to CyberArk Application Identity Manager (AIM)

NOTE: The step are different depending on whether CyberArk Central Credential Provider or Window AIM/AAM Agent are used.

Granting access when using AIM/AAM agent to retrieve secrets

NOTE: The credential provider of the Windows AIM/AAM Agent should also be installed on all TPP engines and should be added as a member of the Safe.

1. Add the credential provider of the AIM/AAM as a Safe Member.

   For example: Prov_<hostname of the machine where AIM/AAM is installed>.

   These provider objects MUST have these permissions to the CyberArk Safe:

   - **Service Account:** Select **View Safe Members** permission and access to the PVWA interface
   - **End user account:** Select **Retrieve accounts** or **Use accounts.**
   - **TPP Application ID:** Select **Retrieve accounts**
   - **Windows AIM/AAM Agent credential provider (Prov_<hostname> one)**: Select **Retrieve accounts**, **List accounts** and **View Safe Members**

2. Click **Save** after setting permissions for each object.

Granting access when using Central Credential Provider to retrieve secrets

1. Add the credential provider of the AIM/AAM as a Safe Member.

   For example: Prov_<hostname of the machine where AIM/AAM is installed>.

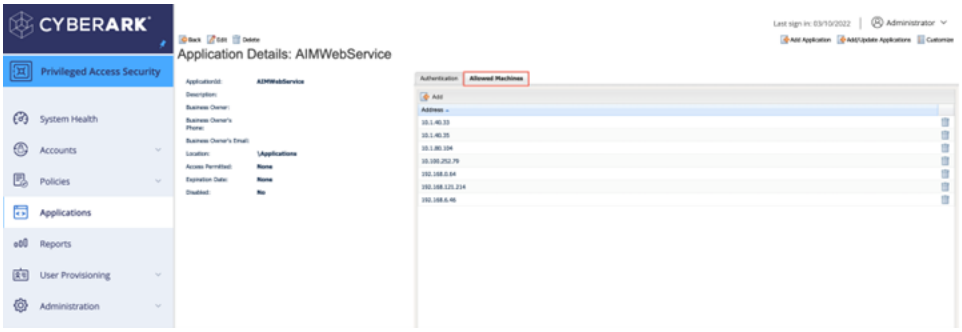
   These provider objects MUST have these permissions to the CyberArk Safe:

   - **Service Account:** Select **View Safe Members** permission and access to the PVWA interface
   - **End user account:** Select **Retrieve accounts** or **Use accounts.**
   - **TPP Application ID:** Select **Retrieve accounts**
   - **CCP credential provider (Prov_<hostname> one)**: Select **Retrieve accounts**, **List accounts** and **View Safe Members**

2. Click **Save** after setting permissions for each object.

If you want to retrieve account secrets in other Safes through the CCP, the same four provider objects must be added as members to the Safes with these same permissions.

3. Add the IP address or FQDN of the machine where you installed the CCP in the **Allowed Machines** tab of the AIMWebService application.



4. The machine where TPP will retrieve CyberArk accounts (secrets) should be allowed to use the TPPApp application in the CyberArk PVWA.

> This can be done by adding the address or hostname of the TPP machine to the **Allowed Machines** tab of the TPPApp created in step 3.

5. On the TPP server the following URL can be used in any web browser in order to test the account (secret) retrieval from the CyberArk Vault (TPP server should be added to the **Allowed Machines** on the TPPApp application)

   https://<CCP Web Sevice URL> /api/Accounts?AppID=<application id>&Safe=<safe name>&Object=<account name to be retrieved>

For example:

https://webservices.example.com
/AIMWebService/api/Accounts?AppID=TPPApp&Safe=TestSafe&Object=test_account

Response:

You should retrieve the account's secret in the response's 'Content' parameter:

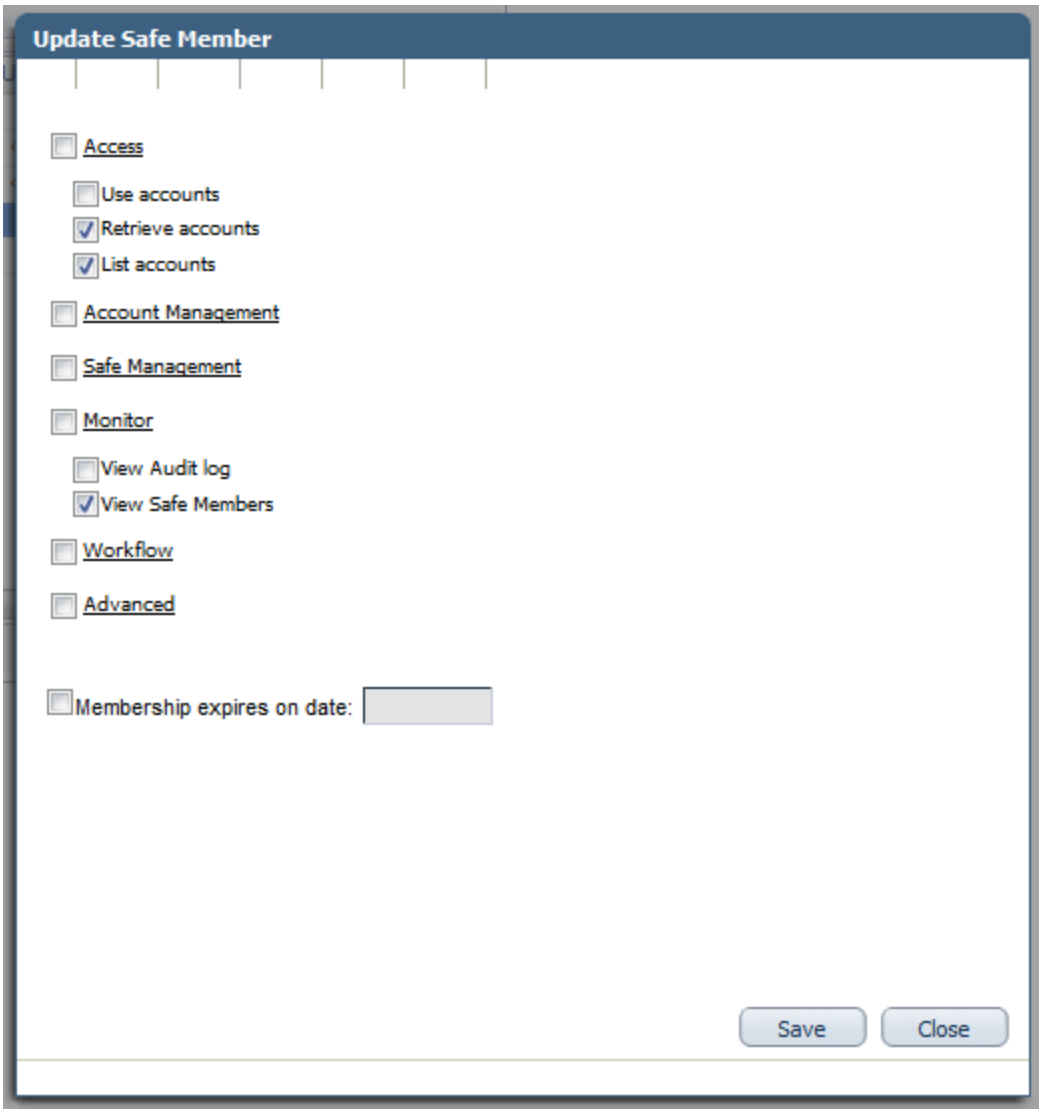
```
{
"Content": "retrieved_password",
"CreationMethod": "PVWA",
"DeviceType": "Network Device",
"Safe": "TestSafe",
"Name": "test_account",
"Folder": "Root",
"PasswordChangeInProcess": "False"
}
```

CyberArk user and password integration requirements

Multiple CyberArk users are needed by Trust Protection Platform when interacting with CyberArk. Use the table below to help you implement the required access in CyberArk.

CyberArk role	Action in Trust Protection Platform	Required CyberArk permissions (for each safe)
End User This is a user created in CyberArk for Trust Protection Platform users who need an application or server to authenticate with CyberArk.	You must provide CyberArk credentials that have access to the safe whenever you create a CyberArk Username Password credential.	*Use accounts* or *Retrieve accounts* **NOTE** User may be granted access individually or via group membership. Access may not be granted using Object Level Access Control (OLAC). A reason cannot be required for the effective Master Policy to access the password for an account.
Application	For Trust Protection Platform to use when it retrieves account passwords from a safe.	*Retrieve accounts*
Authorization User	For Trust Protection Platform to verify that the Actual User is authorized to create Username Password credentials.	*View Safe Members*
Providers	Access required by the Application Identity Manager (AIM) installed on each Trust Protection Platform server.	*Retrieve accounts*, *List accounts*, and *View Safe Members*.

CyberArk's Safe Members permission panel



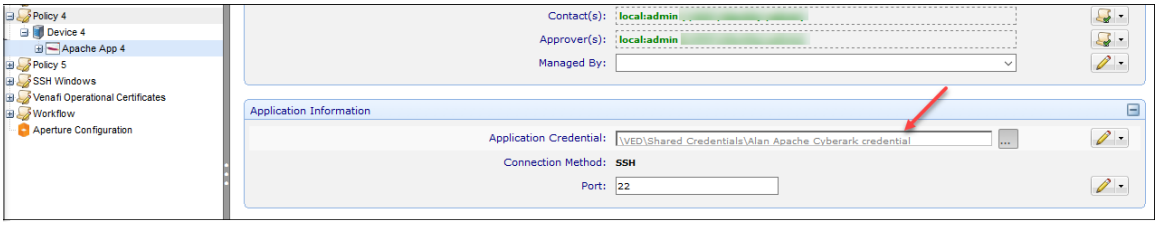
NOTE For information on the settings in the **Update Safe Member** dialog box, please refer to the CyberArk documentation.

Using a CyberArk credential for provisioning (certificate installation)

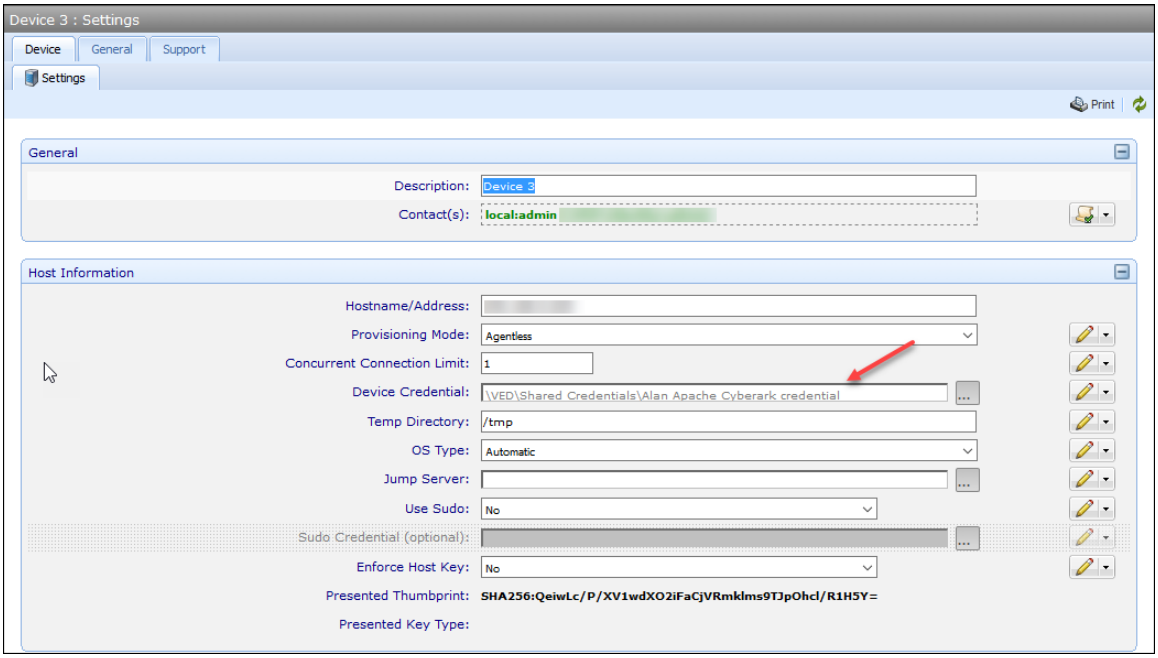
You can use your CyberArk credentials to help secure and speed up the provisioning process. Trust Protection Platform will use the CyberArk credentials you created to access the CyberArk vault and retrieve the correct password.

To use a CyberArk credential for provisioning

- On an application



- On a device

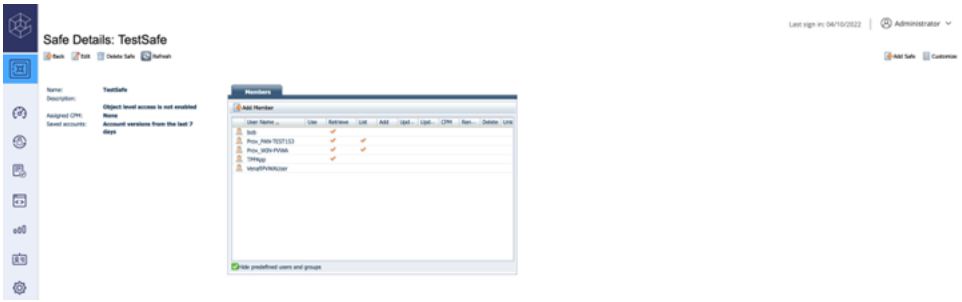


Check CyberArk permissions on safe members

Verify all necessary permissions are added to the safe members

1. Log in CyberArk PVWA and go to **Policies** > **Safes**.
2. Find the safe for which you want to check the permissions and click **Members** .

3. Add or check the members from section **CyberArk AIM/AAM Agent configuration** or **CyberArk Central Credential Provider configuration** depending on the account (secret) retrieval method you are using.



This example illustrates the correct members and their permissions:

- bob is the end user provided in the **CyberArk Username** field on the create/edit CyberArk credential window in Trust Protection Platform
- TppApp is the application provided in the **Application ID** field on the create/edit CyberArk credential window in Trust Protection Platform
- VenafiPVWAUser is the service account provided in the **Web Service User** field on the CyberArk connector in Venafi Configuration Console
- Prov_WIN-PVWA is the Central Credential provider (this member is not needed when using the Windows AIM/AAM Agent retrieval method)
- Prov_PAN-TEST153 is the credential provider of the TPP engine where the AIM/AAM Agent was installed (this member is not needed when using CCP retrieval method)

PowerShell script reference for Adaptable Credential

This section documents all available PowerShell functions for use with the Adaptable Credential driver. You'll find a sample Adaptable Credential script, Template.ps1, in *drive*:\Program Files\Venafi\Scripts\AdaptableCredential\Samples. However, for PowerShell scripts to function, they must be moved into their respective folders: *drive*:\Program Files\Venafi\Scripts*[AdaptableDriver]*.

> **TIP** For more information about reference sample scripts, such as the HashiCorp Vault reference sample, visit the at https://marketplace.venafi.com/.

NOTE To work effectively with any Venafi adaptable solution, you must have some working knowledge of PowerShell scripting, or you must have equivalent experience with a scripting language similar to PowerShell.

The input parameters and response format for each function is predefined. All functions receive a set of general parameters, whereas those parameters that are *specific* to the function are only passed to it.

DID YOU KNOW? To prevent vulnerabilities, the PowerShell scripts are stored on the Trust Protection Platform server. While it might have been more convenient to allow downloading the script, storing the scripts on the Trust Protection Platform server prevents potentially harmful scripts from affecting the server. Only privileged users on your Trust Protection Platform server can access the script.

If you have multiple Venafi Trust Protection Platform servers, you need to ensure your Adaptable Credential scripts are on all servers in the cluster. For this reason, it is wise to include a script version number in the file name, so you can easily check to see that the same version of the script is installed on all servers in the cluster.

Data is passed to the functions using hash tables (key-value pairs). Using hash tables enables the addition of new functions in future releases. For more information, see "About hash tables for Adaptable Credentials" on the next page.

BEST PRACTICE When customizing (or creating a new) PowerShell script, keep the following security best practices in mind:

- Avoid hard-coding credentials into your PowerShell scripts.
- Only include code in functions that relate to the task they are designated to perform.
- Scripts should not do anything that could alter the integrity or availability of the local Windows system (the system hosting Trust Protection Platform).

When you've created your script, learn how to create Adaptable Credentials and put your script to work.

To continue with developing your Adaptable Credential PowerShell script, refer to the following topics:

"About hash tables for Adaptable Credentials" on the next page

"Adding custom fields to your Adaptable Credential" on the next page

"Test-Connector function" on page 970

"Retrieve-Credential function" on page 971

About hash tables for Adaptable Credentials

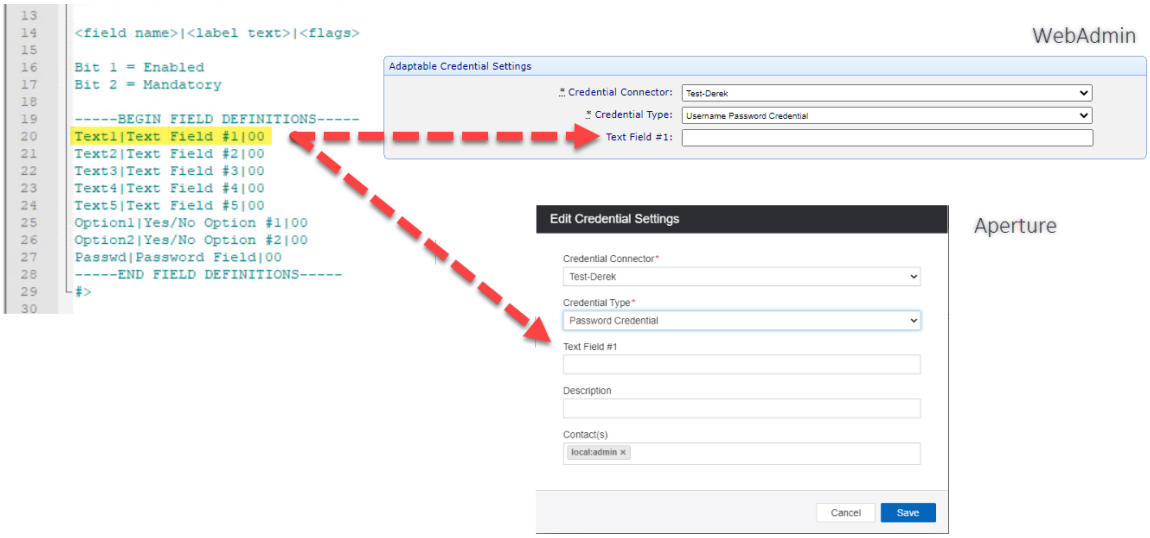
Data is passed to (and returned by) each function using hash table data structures.

A *general* hash table, which includes a common set of data, is passed to all of the functions. A *specific* hash table, which includes data that is applicable specifically to the function, is passed to functions that require additional data. All functions must return a single hash table that includes a *result* along with any other variables that the function is required to return.

Consider the following guidelines and expected behaviors:

Adding custom fields to your Adaptable Credential

The Adaptable Credential provides a common set of variables required connect with third-party passward vaults. However, if your vault requires passing unique or additional data to your script or third-party vault, you can define up to five additional text fields, two yes/no (Boolean) fields, and one password credential field. You do this by simply modifying the **Begin Field Definitions** section of the Adaptable Credential PowerShell script.



Each field definition has three parts:

> *Field Name*| *Field Label*| *Flags*

1. Field Name: Must be `Text1` through `Text5`, `Option1` and `Option2`, and `Passwd`. Do not modify these values.

2. Field Label: Type the name that you want to appear on the Adaptable Credential settings page as they appear in Aperture or Policy Tree.
3. Flags: Using the numeric values of 0 (to mean false) or 1 (to mean true) for each of the following options (in order):
    - Enabled: Use to enable or disable a field.
    - Mandatory: Use to indicate whether the field must be completed, or is optional. When set to true, this option adds an asterisk (*) next to the field label to let the user know that it is a required field.

EXAMPLE Suppose you want to add a field for capturing the user name for the third-party password vault account. Using a text (or PowerShell script) editor, you would open your PowerShell script file and edit the field definitions in the header section to include a new field labeled *Vault Account User Name* and set values for the available flags:

```
----------BEGIN FIELD DEFINITIONS--------

Text1|Vault Account Username|11
Text2|Text2|00
Text3|Text3|00
Text4|Text4|00
Text5|Text5|00
Option1|Create Service|11
Option2|Activate Changes|10
Passwd|API Key|11
```

When you're finished, you save your changes to the PowerShell script. When you open either Aperture or Policy Tree, your new fields appear on the relevant Adaptable Credentials pages.

To create (or edit) Adaptable Credential data fields

1. Open your Adaptable Credential PowerShell file using a text (or PowerShell script) editor.

    IMPORTANT Adaptable Credential PowerShell script files must be stored in the *drive*:\Program Files\Venafi\Scripts\AdaptableCredential folder.

2. Locate the **Begin Field Definitions** section and determine where you want to place your new field.
3. On the line where you want to define your new field (one of the Text or Option lines), type the new field label and then set the appropriate flags.

    For example:

```
Text1|User Name|11
Text2|Password (or Token)|11
```

4. When you are finished, save the file and close it.

Your new field should appear on both the Adaptable Application policy and application object pages in Policy Tree and Aperture.

Test-Connector function

Use the *Test-Connector* function to specify the endpoint URL of the third-party password vault and to pass in required data for authentication.

The following table is part of the General hash table and not separate parameters passed to that function.

Variable Name	Data Type	Description
PfxData	Byte Array	PKCS#12 keystore containing client certificate and private key for authenticating with the third-party vault; this and the PfxPass are used together to instantiate an X509Certificate2 object for client certificate authentication.
PfxPass	SecureString	Password for access to the private key of the PfxData PKCS#12
Username	String	User name for authenticating with the vault
Password	String	The password or Token required for authenticating with the vault
VaultUrl	String	The vault endpoint URL

Return	Data Type	Description
Result	String	Shows "Success" to indicate the non-error completion state, or an error message if unsuccessful

For information about processing stages, see About Certificate Lifecycle Management.

Retrieve-Credential function

Use the *Retrieve-Credential* function to specify the endpoint URL of the third-party password vault and to pass in required data for authentication.

Variable Name	Data Type	Description
PfxData	Byte Array	PKCS#12 keystore containing client certificate and private key for authenticating with the third-party vault; this and the PfxPass are used together to instantiate an X509Certificate2 object for client certificate authentication.
PfxPass	SecureString	Password for access to the private key of the PfxData PKCS#12
Username	String	User name for authenticating with the vault
Password	String	The password or Token required for authenticating with the vault
VaultUrl	String	The vault endpoint URL

Variable Name	Data Type	Description
ConnectorDN	Byte Array	The DN of the Adaptable Credential Connector
CredentialDN	SecureString	The DN of the Adaptable Credential
CredentialType	String	A credential type (string) that the Adaptable Credential object will represent (e.g. "Password Credential", "Username Password Credential", "Certificate Credential", "Private Key Credential", "Amazon Credential")
VarText1	String	Value for the text this custom field defined by the header at the top of your script
VarText2	String	Value for the text this custom field defined by the header at the top of your script
VarText3	String	Value for the text this custom field defined by the header at the top of your script
VarText4	String	Value for the text this custom field defined by the header at the top of your script

Variable Name	Data Type	Description
VarText5	String	Value for the text this custom field defined by the header at the top of your script
VarBool1	Boolean	Value for the yes/no custom field defined by the header at the top of your script (true|false)
VarBool2	Boolean	Value for the yes/no custom field defined by the header at the top of your script (true|false)
VarPass	String	Value for the text password custom field defined by the header at the top of your script

Return	Data Type	Description
Result	String	Shows "Success" to indicate the non-error completion state, or an error message if unsuccessful
Password	String	The retrieved credential password
Username	String	The retrieved credential user name

Protecting against unapproved changes to Adaptable Credential scripts

Venafi's Adaptable drivers– including Adaptable Credential–rely on PowerShell scripts stored in the directory on Trust Protection Platform servers. To ensure the integrity of these scripts, Trust Protection Platform supports signed scripts.

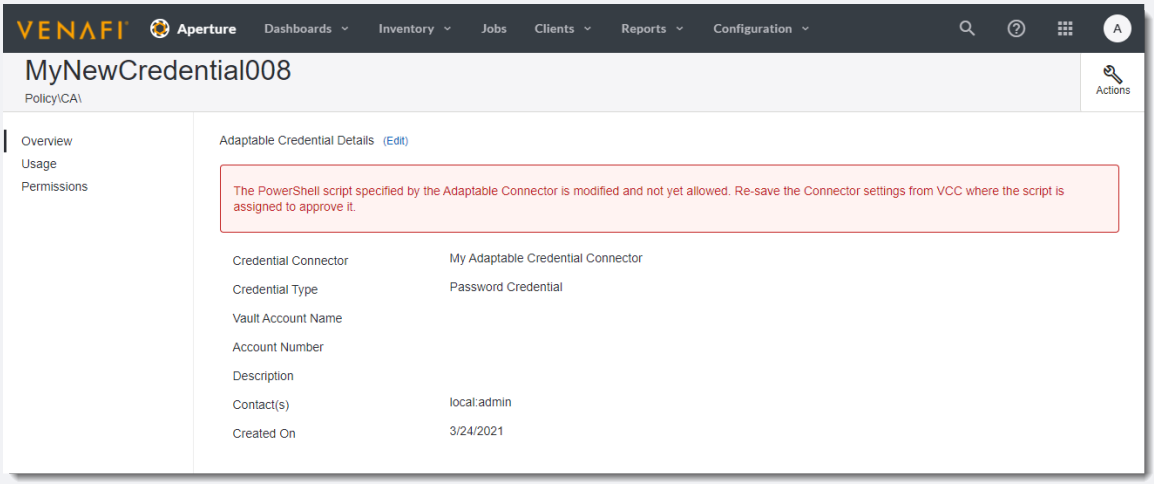
Because other people might have access to the server that is running Trust Protection Platform, they could modify your PowerShell scripts without your knowledge, either accidentally or intentionally. However, with signed scripts, any modifications made to the script will result in a failed signature validation, and the script will not be executed.

To protect against unapproved changes to your scripts, Trust Protection Platform monitors PowerShell script files that are being used by existing Adaptable objects. If a new script is used or a PowerShell script is modified on the file system, Trust Protection Platform displays a warning and you'll need to re-validate the script.

This security feature helps to prevent potentially harmful modifications to your scripts from being run.

EXAMPLE Suppose you updated your Adaptable Credential script by adding two new custom fields to support your new third-party password vault. You save your script changes and open Aperture.

From the Inventory > Credentials page, you apply the Credential Type filter to locate your Adaptable Credentials. You open a credential that depends on your modified script and the following error is displayed:



To get out of this error state, you simply open the Venafi Configuration Console (VCC), open the related Adaptable Credential Connector and re-save it.

In Aperture, you reload the page to find that your Adaptable Credential is functioning normally again.

To safely re-enable an Adaptable Credential following a change to its associated PowerShell script

1. On the Trust Protection Platform server, open and review modified scripts to verify that they contain only approved changes.
2. Open the Venafi Configuration Console, select the Adaptable Credential Connector that depends on the updated script, and then click **Properties** from the **Actions** pane.

3. When prompted about a PowerShell script change, click **OK**.
4. In the **Properties** window, click **Apply** > **OK**.

   All Adaptable Credentials that relied on your script are re-enabled automatically.
5. (Optional) To verify that affected Adaptable Credentials are working again, review them in **Aperture** > **Inventory** > **Credentials**.

   Refer to the EXAMPLE above.

About Generational Management

TLS Protect's Generational Management feature helps to clean up old certificates no longer used by their associated devices while also providing a backup of the certificate on the device.

Generational Management creates and uses *generational credentials* to store the credentials required to remove a certificate and private key after they are replaced. It is a transient credential that is updated every time TLS Protect renews a certificate and private key pair. You do not need to do anything to a generational credential object; in fact there are no configurable options on a generational credential object. They are credentials used simply to ensure that old version of the same certificate can be deleted from a device automatically.

In addition, Generational Management is designed to ensure there is always a backup left on the device—one previous generation of the certificate—so that in the unlikely event that a rollback is necessary, it can be performed quickly by a device administrator and can make use of the same certificate that was known to work previously.

> **NOTE** TLS Protect lets you provide the credentials for the current certificate and private key in the application object's Set/Change menu. (You need to provide the values in the Set/Change menu only if the current certificate and private key were not installed by TLS Protect.)

> **NOTE** It's important to avoid renaming or deleting a generational credential. Doing so could result in the elimination of required data drivers needed for Generational Management. While Trust Protection Platform manages generational credentials automatically, users are cautioned against making manual changes to these credentials.

19

Venafi Trust Protection Platform reports

The Venafi Trust Protection Platform offers a comprehensive suite of reports designed to provide critical insights into your certificate and key management environment. These reports help you monitor, analyze, and respond to potential security risks, ensuring that your organization's encryption assets are secure and compliant. By leveraging these reports, you can detect anomalies, track certificate usage, and maintain a robust security posture.

> **NOTE** Certificates marked as "Processing Disabled" are included in custom reports unless the appropriate filter is applied. This setting does not affect default or "canned" reports.

Trust Protection Platform provides the following default reports.

- The **Certificate Authority Report** contains details related to certificate authorities (CA).

  For detailed information on this report, see Certificate Authority report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Certificate Inventory Report** provides an overview of critical information and statistics about the certificates in your environment so that you can detect anomalies or issues and respond in order to secure and protect your environment.

  For detailed information on this report, see Certificate Inventory report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Certificates with Identical Attributes Report** shows user, device, and server certificates that share an identical attribute with at least one other certificate.

  For detailed information on this report, see Certificates with Identical Attributes report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Entitlement Report** shows all users that have access to the encryption management system.

  For detailed information on this report, see Entitlement report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Expiration Report** contains details about the upcoming expiration dates of your certificates. Expiration dates are displayed from most urgent to least urgent, as defined when the report was generated.

  For detailed information on this report, see Expiration report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Key Length Report** contains details about key lengths of the certificate group you specified. Key lengths are sorted in relative order, from short (weak) to long (strong). This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Key Length report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Licensing Report** provides a count of all managed certificates and their associated applications as well as managed SSH and symmetric keys so administrators can determine if they are in compliance with their current licensing agreement. This report is provided as a default object in the Reports tree because Trust Protection Platform uses the data from the Licensing Report to populate the License Status tab in the administration console Dashboard.

  For detailed information on this report, see Licensing report in the *Venafi Trust Protection Platform Administration Guide*. .

- The **Signing Algorithm Report** contains details related to Digital Signature Algorithms (signing algorithm). The details will help you evaluate risk and company security policy compliance. The algorithms have been sorted in relative order, from weak to strong. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Signing Algorithm report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Validity Period Report** contains shows validity periods for your certificates for the purposes of compliance. The number in the "Years" column reflects the total validity period of the corresponding certificate, not the time remaining. Validity periods are sorted in relative order from long to short, measured in years. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Validity Period report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Wildcard Report** contains details about the use of wildcard certificates. Wildcard certificates are displayed in the table and include the total number of instances and detail associated with each instance. These certificates are sorted by number of instances, from greatest to fewest. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Wildcard report in the *Venafi Trust Protection Platform Certificate Management Guide*.

Managing system reports

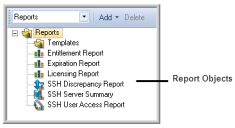
Venafi Trust Protection Platform™ provides reporting functionality so administrators can determine current permissions assignments, view lists of expiring certificates, and review licensing status.

About reports

Trust Protection Platform provides reporting functionality to help administrators more effectively manage their encryption environment.

The Report objects in the Reports tree provide the information that the Reporting module requires to generate each report.

Figure 19.2: Report Objects



- The Reporting module is the program component that generates the reports configured in the Reports tree.

IMPORTANT You must configure the Reporting module before Trust Protection Platform can generate reports and populate the Licensing tab in the Dashboard.

- The Reporting module is located in the Platforms tree. For information on configuring the Reporting module, see "Configuring the Reporting module" on page 852
-  The Root Report object contains all other objects in the Reports tree. When you configure the Root Report object, you can define the default permissions that are inherited by all subordinate Report objects. For more information, see "Configuring the root report object" below.
-  The individual Report objects determine report format, how often the report is generated, and report delivery options. For more information, see "Venafi Trust Protection Platform reports" on page 975.

Configuring the root report object

The Policy Tree Root Report object contains all other objects in the Reports tree. When you configure the Root Report object, you can define the default Contact and permissions that are inherited by all subordinate Report objects.

The following table describes the available settings and options for the root Report object.

Field	Description
Report Root Tab	
Description	Custom description for the Root Report object.
Contact	User or group Identities assigned to this object.Default system notifications are sent to the contact identities. Default contact = master administrator **To select the object contacts** 1. Click the **Browse** button. The Identity Selector dialog opens.

Field	Description
	2. If the Identity Selector dialog is not populated, enter a search query to retrieve the Identity list. The administration console does not automatically display external users and groups. You must first enter a search string so Trust Protection Platform can query the external Identity store and return the list of requested users or groups.If you want to display all user or group entries, enter the wildcard character (*). 3. Select a User or Group Identity, and then click **Select**. 4. Press **Shift+click** to select multiple, contiguous users and groups. Press **Ctrl+click** to select multiple, discontiguous users and groups.
General Tab	
Log	Provides a view of all events triggered for the current object. An administrator must have a minimum of the Read permission to view this tab.
Permissions tab	On the Permissions tab, you select the users or groups to whom you want to grant permissions to the current object. Then, you select which permissions you want the users or groups to have. You can also manage object permissions via parent objects, including the root Platform object or the Trust Protection Platform server object (found in the Platforms tree). If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Creating reports in the Policy Tree

As with most objects, make sure that you have the *Create* permission to the root Report object before completing the following procedure.

To create a report in the Policy Tree

1. From the TLS Protect menu bar, click Policy Tree.
2. Select the **Reports** tree from the Tree drop-down menu.
3. In the Reports tree, select the root Report object, and then click **Add**.
4. Select the type of report you want to create.
5. Type a name for the report, and then click **Create**.
6. Define the Report object settings.
7. Click **Save**.
8. Click the **Setup and Delivery** tab and **Schedule** tab for additional options you can configure for delivery of reports.

   In particular, note the **Skip delivery if no report data is generated** option on the **Setup & Delivery** tab. If this option is *not* selected, a report will be generated and delivered even if no data is in the report. We recommend you select this option to reduce the delivery of unnecessary (and unhelpful) empty reports.

Manually generating reports

This topic shows you how to generate reports manually instead of on a fixed schedule.

Although administrators may configure a report to generate on a scheduled basis, they can also manually generate a configured report as needed. In fact, if administrators prefer not to generate reports on a regular schedule, they may manually generate reports whenever they want to canvass their certificate environment.

A manually generated report is generated and distributed according to the Setup & Delivery options configured in the Report object.

To manually generate a report

1. From the TLS Protect menu bar, click **Policy Tree**.

   NOTE You must have the View and Write permissions to the report.

2. Select the Reports tree from the Tree drop-down menu.

3. In the Reports tree, select the report, then select the Report tab.
4. On the Report tab, click **Run Now** 

The report is placed in the Report engine queue. After you initiate the report generation, the **Run Now** option is not available until after the Report engine completes the report.

When the Report engine generates the report, it formats and distributes the report according to the parameters configured in the Report object's **Setup & Delivery** tab.

After Trust Protection Platform generates the report, you can also download the report from the Report object's Report tab.

To download the report

1. From the TLS Protect menu bar, click **Policy Tree**.

   NOTE You must have the View and Write permissions to the report .

2. Select the Reports tree from the Tree drop-down menu.
3. In the Reports tree, select the report, then select the **Report** tab.
4. On the Report tab, click the Download button  .
5. Select the available format.
6. In the **Save Report** dialog, browse to where you want to save the report, and then click **Save**.

20

Understanding system logging and notifications

With Venafi Trust Protection Platform™, you're not just monitoring and managing your encryption resources—you're also keeping track of those activities and passing along important information about system events as they occur. The platform's log server monitors events and centralizes the logged information. This makes it easier for you to review and assess how your encryption system is performing. Whether you're auditing, troubleshooting, or conducting operational reviews, these logs are your go-to resource.

You can also configure notifications for specific events. By defining notification rules, you can route information about events to a variety of channels like SMTP, SNMP, File, MS SQL, or Sysog, keeping you updated about the events you care about in whatever formats you choose.

Logging system overview

The Trust Protection Platform logging system consists of the following components:

- **Events**: Describe an error or status. For example, an event fires when a certificate is about to expire.
- **Venafi log server**: Monitors events, processes logs, and manages sending alert information to specified destinations.
- **Default SQL Channel** : Stores a history of events as a log to a database. These logs can be filtered using a Filter Channel to reduce unwanted or unhelpful event logs.

- **Notification Rules**: Determine which events are forwarded to channels for processing and which events are ignored.
- **Channels**: Manage the delivery of processed log messages in a variety of formats.

For more information, see "Understanding system logging and notifications" on the previous page in the *Log Server Administration Guide*.

Log events

Log events are generated by Trust Protection Platform components as well as custom add-ons provided by Venafi, our partners, or customer organizations.

All log events have a standardized set of fields. This allows the log server to store events in a database and query events across all sources.

When an event occurs, the following sequence of events beings.

1. A Trust Protection Platform component serves an event to the Log API.
2. If the event's severity level is `Debug`, and the Debug setting is disabled, it is discarded.
3. The Log API sends the event information to the MSSQL Service Broker Queue for processing.
4. The log server periodically checks the queue.
5. The log server sends the event to the default log channel.
6. The log server applies matching notification rules. This may trigger sending the event information to the corresponding channels.

A

Appendix A: Enabling Demo Mode

Trust Protection Platform includes a setting called *Demo Mode* that was originally designed to make it easier and faster to demonstrate how the product works. Demo Mode reduces the intervals that the system normally waits to perform certain actions, like how often Discovery checks for work. This is beneficial if you are testing the system, training users on how to use the system, or doing troubleshooting tasks that would work faster with the reduced intervals.

> **WARNING!** Demo Mode is not intended for production systems. It should not be used in environments with large data sets. It is intended for demoing and testing purposes only.
>
> While the intent of Demo Mode is to increase the responsiveness of the system, this setting will cause problems if there is more data in the system than the system can process during the shortened intervals, which can lead to system instability.

To enable Demo Mode

1. On the Trust Protection Platform server, open the registry editor and browse to the following location:

   ```
   HKEY_LOCAL_MACHINE\Software\Venafi\Platform
   ```

2. Click **Edit** > **New** > **String Value**.

3. Type the following:

   ```
   Demo Mode
   ```

4. Type the following value in the **Data** column:

```
Enabled
```

5. Close the registry editor.
6. Repeat the previous steps for all Trust Protection Platform servers in the cluster.
7. Restart the running services in the Venafi Configuration Console.

If you decide later that you want to disable Demo Mode, update the registry key to the following data value:

```
Disabled
```

B

Appendix B: Venafi Data Privacy Policy for Venafi Trust Protection Platform™

Effective: July 1, 2019 (v19.2)

When you use Venafi Products and services, we know you are trusting us with your information. We understand that this is a big responsibility and work hard to protect your information. This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how we use this information. It also describes what controls are available to you and how you can request that your information be deleted and not tracked any more.

Types of information we collect

We collect information to provide better products and services to you, our customer, including retrieving diagnostic and performance information to improve product stability and scalability.

Your installation of Venafi Trust Protection Platform

We collect non personally-identifiable information about your deployment of Venafi Trust Protection Platform. Information like the version history of your deployment, the operating system it is installed on, the SQL Server version used to host the database. We also collect information on the products that are installed/enabled on the platform as well as the license levels consumed. Other items we collect include your Organization name, the type of deployment, the number of Venafi servers deployed, and which features are and are not being used.

How we use the information we collect

We use data to build better products and services to do the following things.

Provide our services

We use non personally-identifiable information to enhance our products and services, like providing notifications of newly available patches and major releases or providing in-app contextual help on new features.

Maintain & improve our services

We also use non personally-identifiable information to ensure our products and services are working as intended, such as tracking platform instability, troubleshooting issues, and making improvements to our products in future releases (such as improving navigation in the product or simplifying the process for requesting a certificate).

Measure performance

We use non personally-identifiable aggregate data for analytics and measurements to understand how our products and services are used. For example, we may analyze data about the performance for dashboard load times, inventory list load times, or how long it takes to perform a network discovery job. This information helps us know where we need to invest in making the product faster and more scalable.

How we use cookies in our products

What is a Cookie?

Cookies are a standard feature of websites and web applications that allow us or our partners to store small amounts of data on your computer about your visit to the website or service. Cookies help us learn which areas of the site or application are useful and which areas need improvement.

You can choose whether to accept cookies by changing the settings on your browser. However, if you disable this function, your experience when using Venafi products and services may be diminished and some features may not work as intended.

All the cookies we use are safe for your computer. They store only small amounts of data, which is stored by your web browser. Our cookies do not track or collect your personally-identifiable information, do not run code, do not contain malware or viruses, and cannot access any other data on your machine. The purpose of cookies is to allow us to provide you a better, and sometimes faster, browsing experience.

What Cookies does Venafi use?

We use cookies and IP tracking codes to collect non personally-identifiable aggregate data for statistical purposes, and to enhance our understanding of how you interact with our product.

How long we store the information we collect

We will store the information we collect for as long as is necessary and relevant to our providing our services to you. If you terminate your subscription or close your account, we may still retain your non personally-identifiable information for analytical and historical reporting purposes, troubleshooting problems, as well as to comply with any legal requirements. We will store this information as long as we are legally allowed to, at which point we will delete the data.

For question about this privacy policy, contact privacy@venafi.com.

How we use cookies in our products

C

Appendix C: Open Source Information

To see what open source libraries are used in Trust Protection Platform, see https://docs.venafi.com/25.1/open-source.

.

.NET environment template 212

#

3DES 572

128f 572

128s 572

192f 572

192k1 572

192r1 572

192s 572

224r1 572

256d 572

256f 572

256r1 572

256t1 572

320r1 572

320t1 572

384r1 572

384t1 572

512t1 572

2048 572

3072 572

4096 572

8192 572

A

access grant 765

access grant expiration 765

access grant validity 765

access management 153, 389

accessibility 757

accident 138

accidentally 138

account preferences 7, 12, 631-632

account settings 12, 631-632

ACME 68, 844

certbot 68, 844

ACME Server Settings tab 768

ACME Server tab 768

active directory 96, 638, 643, 645

Active Directory 655, 672

Active directory

deleting 670

active directory configuraiton 643

active directory settings 643

AD 672

AD configuration 643, 655

Adaptable App

prerequisites for using 313, 467

Adaptable Application

editing policy settings for 878

Adaptable Credentials configuration 95

Adaptable Credentials Driver 95

Adaptable Log Channel 313, 467

about hash tables 324, 478

configure 318, 472

log expiring certificates 317, 471

Perform-Action function 324, 478

protect from unapproved PowerShell script changes 321, 475

script 314, 322, 468, 476

ServiceNow example 317, 471

add license 75

administration consoles

Trust Protection Platform user interfaces 3

Advanced Key Protect 106, 580-581, 585, 588, 590

AES 572

agent api 70, 846

agents
search filter
how it works 932
algorithms 56, 573-574
algorithym configuration 56, 574
All Certificates Dashboard 599
allowed algorithms 56, 573-574
allowed encryption 56, 574
Allowed Outbound SSL/TLS Versions 768
allowed signing applications 249
AlwaysOn Availability Groups 293, 447
Amazon
authenticating with Trust Protection Platform 942
Amazon Credential 940
Amazon credential
EC2 Assigned Role 941
Amazon Web Services
Managed Microsoft AD 636
ambiguous identity 137, 837
analytic data 4
analytics 4
answer file 46
answer file wizard 46
Apache 590
Apache remote key generation 590
Aperture
about responsive layout 5
about switching between dashboards 5
unified menu bar 5
working in 14
aperture 5
Aperture Global Search
about 5
aperture menu 5
Aperture User Search
enabling 745
api access 153, 389
API access 763
api access management 153, 389

API Integrations 756
about 750
creating 752
deleting 760
exporting 761
revoking grants and tokens 760
API Integrations inventory 756
API session 765
Applications
policy settings for 878
approval 10
approval list 10
approval request 10
approval type 10
approvals 7, 10
approvers 198
asymmetric 570
asymmetric algorithm 570
asymmetric encryption 570
Authentication 109, 768
authentication 113, 813
alternate options 791
single sign on 791, 809
SSO 809
Authentication Settings tab 768
authhentication credentials 96, 638
automatic cleanup 145
automatic credential rotation 61, 356
automatic delete 138, 145, 147
automatic deletion 147
Automatic Layout Manager 68, 844
automatically delete 145
available algorithms 573
available encryption 573
AWS
authenticating using a single Amazon Credential 942
Azure Active Directory connection requirement 636

B

brainpool 572

browser based authentication 764

Bulk Provisioning 69, 845

Bus Health Issue 263, 415

C

CA import 69, 845

CA templates 181

- DigiCert 184
- Entrust 187
- Microsoft 191
- Microsoft pool 193
- self-signed 195

caching 765

call home 4

CAPI 593

CAPI remote key generation 593

CDP 69, 845

central key generation 580

Central MQTT broker 257, 409

certificate authentication 764

certificate authorities

- approving 602, 610
- tracking 600, 615
- unapproved issuer 602, 610

certificate cleanup 146

certificate credential

- create using Policy Tree 927
- creating 912
- viewing all properties 933

certificate credential configuration 918

certificate credential object 918

certificate environment template 207, 210

certificate expiration

- tracking 600, 616

certificate installation 590, 593-594

certificate lifecycle 69, 845

Certificate Manager Settings tab 768

certificate trends
tracking 605, 616
certificate validity period 607, 615
Certificate Verification 839
Certificate Verification Settings 768
certificates
authentication 793-794
protection level
none assigned 601, 615
search filter
how it works 932
change management flows 203
change timeout 110
channel
configuring 291, 294, 445, 448
configuring MS SQL 289, 443
creating channel objects 288, 442
Default SQL 297, 451
email configuration 297, 451
File 327, 481
Filter 332, 486
for email 296-297, 450-451
MS SQL 291, 445
notification 285, 439
requirements 290, 444
SMTP 296-297, 310, 450-451, 464
SNMP 334-336, 339, 488-490, 493
SQL 294, 448
templates 297, 451
channels
configuring 288, 442
email configuration 288, 442
SMTP 288, 442
syslog 340, 494
Cipher 540
classic policy tree 17
cleanup 145-146
cleanup schedule 146
CLI command attributes 61, 356
Client API 70, 846

Client Protect menu 5

Code Signing Administrator 254

Code Signing Client Distribution 71, 847

Code Signing Key Server 71, 847

CodeSign Protect 5

command line configuration 511

command-line interface 61, 356, 511

Common Criteria 542

complex encryption systems

using multiple policy structures 872

configuration 44, 64

Venafi Platform 44

configuration console 58, 60, 64, 76, 359-360

configure allowed algorithms 56, 574

configuring

Trust Protection Platform server 767

connectors 76

consoles

Aperture, customizing 15

Web Admin 17

controller selection 96, 638

create groups 702

create team permission 745

Creating a custom SQL log channel 294, 448

creating credentials 912

using Policy Tree 927

creating private key credential 916

creating user name or password credentials 913

credential

delete 940

credential objects

creating in Policy Tree or Aperture 912

securing 911

credential rotation 61, 356

credentials 61, 253, 356, 937

about managing system 909

certificate credential properties 933

create using Aperture 927

creating 912

creating credential objects 912
CyberArk 944
deleting 940
exploring assigned permissions 937
exploring details 933
generic credential type 925
managing 929
moving to another folder 939
object hierarchy 911
viewing details about specific 929
viewing inventory 929
viewing usage of a specific credential 936
credentials inventory
about 929
filtering 929
CRL 69, 839, 845
CRL Distribution Point 69, 845
CRL Verification 768
Cryptoki 85, 562
CSR key generation 581
custom field 905
macro for notifications 905
custom fields 902, 906
adding or deleting 893
creating a list 897
editing 900
filtering 901
overview 891
reporting on 903
custom log 294, 448
custom menu 6
custom product menu 6
custom SQL log database 294, 448
customer experience improvement 4
customer experience improvement program 4
customize
Aperture console 15
customize menu 6
customized 6
customized menu 6

CyberArk

editing credential 959

CyberArk configuration 101, 951

CyberArk credentials

creating 958

CyberArk Credentials application object 44

CyberArk Credentials Driver 101, 944, 951

for provisioning 964

integration with Trust Protection Platform 944

permissions required 963

CyberArk Enterprise Password Vault

integration with 944

CyberArk Password credential

creating 912

CyberArk Username Password credential

creating 912

CyberArk Web Service

editing the credential 959

D

Dashboard

Aperture

All Certificates Dashboard 599

SSH Keys Dashboard 618

System Status Dashboard 629

User and Client Device Certificate Dashboard 610

Widgets See Widgets

database 44, 58, 60, 359

connection type 58

custom SQL log 294, 448

encryption 293, 447

repair connection 60, 359

system requirements for using Oracle Access Manager 810

database connection string 59

default algorithm 56, 574

default algorithms 573

default containers 171

default encryption 56, 574

default page 6

delete 138

deleting credentials 940

deleting enviornmnets 203

deleting projects 203

deletion task 145-146

Demo Mode

enabling 985

Demonstration Mode

enabling 985

DES 572

digest algorithms 566

DigiCert CA template 184

digital signature 566

disable rediscovery 98, 641

Discovery Zones 768

domain controller 672

Domain Selection 96, 638

DPAPI key 76

back up or restore 77, 554

DSA 572

E

EC2 instance

using with Amazon credentials 941

ecdsa 572

ecp 572

edit Message Bus 257, 409

editing credentials 937

elliptic 572

Email

configuration 106, 281, 435

notifications 106, 281, 435

setup 106, 281, 435

email

configuration 297, 451

email notifications 297, 451

HTML-formatted 298, 452

plain text 298, 452

enable rediscovery 98, 641

encryption 56, 85, 562, 573-574

database 293, 447

encryption algorithms 566

Encryption Driver

overview 546

encryption keys

using HSM-protected 557

validating 566

Entrust CA template 187

environment templates 207

.NET 212

apple 210

certificate 207

edit 248

GPG 215, 222, 233, 237, 244

key pair 219

error codes

list of 271, 424

event 271, 424, 984

configuring event log retention 353, 507

File channel 327, 481

Filter channel 332, 486

for email 296, 450

SMTP channel 296-297, 450-451

SNMP channel 334-336, 339, 488-490, 493

SQL channel 289-291, 443-445

syslog channels 340, 494

event definitions 271, 424

Event IDs

list of 271, 424

event log

size 280, 434

event storage 266, 418

events

viewing 272, 276, 425, 430

exclude from automatic deletion 147

exclude from recycle bin 147

exclude policy folders 147

expiration mode 765

expire session 110

expiry notification 12, 632

export API 761

export integration 761

external identity 672, 688

F

failover 291, 445

File channel

configure 329, 483

requirements 329, 483

filter 761

Filter channel

events 332, 486

Filter Channel object

configure 333, 487

filtering 746, 761

finding identities using filters 740

filters 761

fix HSM pin 360

Flows 175

Global 175

flows 196

configure change management flows 203

configure code signing flows 198

folders

see "policies" 878

FQDN 775

G

generating reports

using Web Administration Console 980

Generational Credential

see Generational Management 974

Generational Management

about 974

Generational Thumbprint

about 974

generic credential type

about 925

getting started
adding objects 28
deleting objects 31
filtering Tree view 37
moving objects 33
renaming objects 36
global catalog 96, 638, 672
Global Options(Impacts all users) 768
global properties 170
global rediscovery 98, 641
global rotation 83
GPG environment template 215, 222, 233, 237, 244
grants
revoke 700
group identities 702, 705
group permissions 721, 739
adding the master admin role 710
groups 705
Groups
setting permissions for 734

H

hardware central key generation 581, 585
hardware encryption key 546
hardware key 76, 85, 562
hardware key generation 581
hardware remote key generation 581, 588
hash function 570
hash tables
about 324, 478
hashing 570
heartbeat triggers 347, 501
HMAC 540
home page 6
host name 775
HSM 76, 83, 85, 360, 562, 578, 580
configuration 85, 562
encryption key 546
migrate key references 88
remote key generation 588

rotation 83

using to protect encryption assets 557

HSM Backend 71, 847

HSM pin rotation 62, 356

HSM-based remote key generation 106, 580, 588, 590

HSM-protected keys 588

managing applications using 588

HTTP

configuring proxy 787

using a proxy 784

HTTP proxy

setting up 787

HTTPS

manually enable in IIS 537

HTTPS connection checking 839

hub and spoke mode 257, 409

I

identities 746

about 635, 674, 677-678, 686-688

about working with identities, permissions, and roles 635, 674, 677-678, 686-688

create 696, 702

external

permissions 672, 688

groups 702, 705

local 696, 698

configuration 698

create 696

permissions 672, 688

managing in Trust Protection Platform 635, 674, 677-678, 686-688

searching for users,groups, and roles 635, 674, 677-678, 686-688

third-party data providers 635, 674, 677-678, 686-688

using filters to find users, groups, or roles 746

using filters to search for identities 740

viewing details about 747

identity 746

revoke grant 700

identity connectors 645, 670

identity driver 645, 670

identity inventory 746

identity permissions 724

identity properties 657

identity provider 655

Identity providers selector 672, 688

identity sharing 672, 688

ignore recycle bin 147

IIS status 64

inactivity 110

inactivity setting 110

inactivity timeout 110

Installation 64

installation

- ACME Service component 67, 843
- Aperture component 67, 843
- Automatic Layout Manager component 67, 843
- Bulk Provisioning component 67, 843
- CA Import component 67, 843
- Certificate Lifecycle and Monitoring component 67, 843
- Client REST component 67, 843
- components available 67, 843
- HSM Backend 67, 843
- Network Device Enrollment component 67, 843
- Network Discovery component 67, 843
- Object Monitoring component 67, 843
- Onboard Discovery Manager component 67, 843
- Reporting component 67, 843
- SSH Key Detection and Remediation component 67, 843
- User Pre-enrollment component 67, 843
- Validation component 67, 843
- Web SDK component 67, 843
- WebAdmin component 67, 843

instrumentation 4

integrated authentication 764

integrated MS Windows authentication 764

invalidsignatureexception 133, 833

inventory 756

inventory accessibility 757

J

JKS 594

JKS remote key generation 594

join a team 692

K

Key exchange 540

key exchange 566

key generation

HSM-based remote 588

key lengths

identifying via SSH Dashboard 621

tracking use of 600, 614

key pair environment template 219

key size 12, 632

keyboard navigation 757

keyboard shortcuts 757

keys

search filter

how it works 932

L

LDAP 655, 657, 661, 672, 688

deleting 670

LDAP connection 657

legacy algorithms 566

license 75

local identity 672, 688

local user directory

managing 694

lockout 657

Log applications 266, 419

log applications 275, 429

Log Channel connector 106, 281, 435

Log events 271, 424, 984

log events

setting time to expire 280, 434

viewing 276, 430

Log Server 265, 418

channel 296-297, 310, 327, 334-336, 339, 450-451, 464, 481, 488-490, 493

configuring event log retention 353, 507

configuring MS SQL channel 289, 443

configuring SQL channel 290, 444

default SQL channel 289, 443

events 264-265, 416, 418, 983

File channel 329, 483

Filter channel 332, 486

maintenance 275, 429

MS SQL channel 291, 445

notification rules 348, 502

notifications 264, 347, 416, 501, 983

Service

stop 278, 432

syslog channels 340, 494

Log Server object 265, 418

configure 279, 433

Log Server Service

start 278, 432

Log store 266, 418

logging

clearning out the log 280, 434

minimizing log event clutter 280, 434

system overview 983

Logging 768

logging in

Aperture 5

Venafi Consoles using the Product Switcher 5

logging in to WebAdmin 17

Logging tree

overview 264, 268, 416, 421

login failure 353, 507

login notifications 353, 507

login screen

customizing 15

Logout 138, 838

Logout SAML 138, 838

Logout SSO 138, 838

M

main menu 5

manage components 64

manage filters 761

manage saved filters 761

master admin

viewing if a user account is granted permissions for 711

master admin role

about 708, 713

adding to a user or group 710

master administrator

about 713

md2 572

md5 572

menu 5-6

menu bar 5-6

menu permissions 6

mesh mode 257, 409

Message Bus 255, 257, 260, 407, 409, 412

Message Bus configuration 257, 409

Message Bus MMC snap-in 255, 260, 407, 412

Message Bus snap-in 260, 412

Message Bus status 260, 412

MIB file 339, 493

Microsoft Azure

private key generation 581

Microsoft CA template 191

Microsoft Pool CA template 193

Microsoft SQL

about channel configuration 289, 443

channel object configuration 291, 445

MMC snap-in 143, 255, 260, 407, 412

modify Message Bus 257, 409

Monitoring 73, 849

moving credentials 939

MQTT 255, 257, 407, 409

MQTT broker 255, 257, 407, 409

MQTT mesh mode 257, 409

my account

my teams 7

My Account 8

N

native generation 581

native key generation 581

nCipher HSM 557

network device enrollment 72, 848

Network Device Enrollment Settings tab 768

Network Device Enrollment tab 768

Network Discovery 73, 849

network requirements for Message Bus 255, 407

notification configuraiton 106, 281, 435

notification rules 347-348, 501-502

notification setup 106, 281, 435

notifications 285, 347, 439, 501

log 285, 439

login 353, 507

SMTP 312, 466

using regular expressions in 353, 506

O

object hierarchy

system credentials 911

objects

search filter

how it works 932

OCSP 69, 845

Onboard Discovery 73, 849

Operations 768

options 172

Oracle

create directory service provider 648

Oracle Access Manager 768

system requirements for using 810

outbound SSH 540

outbound SSL 771

outbound TLS 771

P

password credential
create using Policy Tree 927
creating 912-913
passwords
changing local 700
requirements 700
PBE 572
Pendo 4
Perform-Action
Adaptable Log Channel PowerShell function 324, 478
permissions
about 635, 674, 677-678, 686-688, 713
about permissions and inheritance 716
about permissions for identities 721
about roles 635, 674, 677-678, 686-688
about user 713
administrator 730
Aperture 721
assigned to a credential 937
assigning to object 734
associate 728
create 727, 768
delete 728
enabling Aperture User Search 745
manage policies 728
Policy Tree 739
private key read 729
private key write 730
read 725
rename 728
revoke 729
setting on Agent work 734
setting on Groups 734
SSH 722
view 725
viewing user entitlements 714
write 725
permissions granted 721

personalize 6

personalize menu 6

phone home 4

Ping One 131, 831

PingOne 131, 831

PingOne for Enterprise 131, 831

PKCS#11 85, 562

pkix 56, 574

placement jobs 68, 844

platform connectors 645

Platform menu 5, 509

Platforms Settings tab 768

policies 860

- configuring 878
- configuring subordinate objects 888
- how they work 860
- using multiple structures 872

Policy Tree 18

- using 18

policy tree

- searching 38

port 1883 255, 257, 407, 409

port 8883 255, 257, 407, 409

port assignements 257, 409

post-quantum 566, 570

post-quantum support 570

PowerShell script

- unapproved changes to 321, 475

PowerShell script function

- Perform-Action (Adaptable Log Channel) 324, 478

preferences 8, 12, 632

preferences menu 6

private key credential

- change private key 938
- creating 912, 916
- replacing private key 938

Private Key Credential 917

private key generation 581

private key generation and storate 171

private keys

remote versus central key generation 581

product license 75

product menu 6

Product Switcher

about 5

Proxy Settings 768

Proxy tab 768

PSS 572

public key

not displayed 933

Public Keys

supported for outbound 540

purge 138, 149

purge all 149

Q

quantum 570

quantum safe algorithm 570

quantum-safe 570

quantum-safe algorithm 570

Query mode

start Web Administration Console in 41

query mode 41

R

recycle 138, 143, 145

recycle bin 138, 143, 145

Recycle Bin 138

recycle bin configuration 145

recycle bin options 145

rediscovery 98, 641, 645-646

disable 98, 641, 646

enable 98, 641, 645

refresh recycle bin 150

registry

see Windows Registry 985

regular expressions

using with notification rules 353, 506

remote access 763

remote access configuration 763

remote access tree 763

remote generation 581, 590, 593-594

remote key generation 580-581, 588, 590, 593-594

HSM-based 588

remote key generation settings 590, 593-594

repair HSM 360

report objects

creating in Web Administration Console 979

reporting 73, 849

Reporting connector 106, 281, 435

reporting module 852

reports 975

available 975

configuring root object 978

creating report objects 979

custom fields report 903

manually generating reports 980

Web Administration Console

about the Reports tab 19

request in progress message customization 172

request instance identification 178

reset password 9

reset settings 9

restore 138

revocation 69, 845

revocation checking 69, 845

enabling 69, 845

Revocation Checking 768

revocation monitoring 69, 845

roles

about 706

about working with identities, permissions, and roles 635, 674, 677-678, 686-688

assigned to a specific user or group 747

root report objects

configuring 978

rotate encryption keys 578

rotate system key 83

RSA 572, 797

authentication 791

enabling 802

S

SafeNet Luna SA HSM 557

SAML 109, 113, 135, 813, 835

SAML authentication failed 133, 833

SAML configuration 109, 113, 775, 813

SAML logging 135, 835

SAML Response 136, 836

SAML Response signing 137, 837

SAML troubleshooting 135, 835

saved filters 761

saved searches 761

search 761

user 745

search roots selection 96, 638

searching 761

secondary log channel 294, 448

secondary log sql channel 294, 448

secondary sql log channel 294, 448

self-hosted 257, 409

self-hosted MQTT 257, 409

self-signed CA template 195

services

starting or stopping 64

session 110

session cache 765

session expiration 765

session expire 110

session pool size 765

session timeout 110

set default page 6

set home page 6

Settings 768

Settings tab 768

SHA2 572

SHA3 572

SHA256 572

SHA512 572

Shake 128 572

signing algorithm 12, 632

single sign-on 809

Oracle Access Manager 810

single-sign-on 109

skip delivery report 979

SLH 572

SMTP 106, 281, 435

communication 310, 464

delivery failures 312, 466

SMTP configuration 106, 281, 435

SMTP Default Connector 106, 281, 435

snap-in 143

software central key generation 581

software connector 546

software encryption key 546, 578

software key 76

software key generation 581

software remote key generation 581

SQL connection string 59

SSH 73, 849

account preferences 13, 633

Network Discovery Key Lengths widget 622

Network Discovery Summary widget 623

SSH Certificate 73, 849

SSH key algorithm

tracking 620

SSH key lengths

tracking 622

SSH Keys Dashboard 618

SSH keyset permissions 722

SSH Network Discovery Key Lengths widget

customizing 623

SSH Protect menu 5

SSL 3.0 771

SSO 109, 113, 809, 813

SSO configuration 109, 113, 131, 775, 813, 831

support large object trees 41

symmetric 570

symmetric algorithm 570

symmetric encryption 570

syslog channel

about 340, 494

configuring 343, 497

requirements 342, 496

system cleanup 145

system notifications

specifying recipients 697

system requirements

CyberArk 944

System Status Dashboard 629

T

team approvals 10

team permissions 745

teams 692, 746

teams management 692

threshold 631

time constraint 248

time stamp service 74, 850

time stamping 74, 850

timeout 110

timeout setting 110

TLS 1.0 771

TLS 1.1 771

TLS 1.2 771

TLS 1.3 771

TLS Protect menu 5

token expiration 765

token validity 765

tppconfig 511

tppconfiguration 511

tppconfiguration.exe 511

transport component

failed 543

trash 138

Tree view

in WebAdmin 19

troubleshooting 135, 835

manually enable HTTPS in IIS 537

Trust Protection Platform
configure server object 767
configuring 44
HTTPS 535
SSL 535
trust anchor for 535
Trust Protection Platform URL HostNames 768
Trust Store Management 768

U

undelete 138
undo 138
url host name 775
url hostname 775
urlhostname 775
usage statistics 4
usage statistics, collecting 4
usage tracking 4
user
search 745
User and Client Device Certificates
Dashboard 610
user directory
filtering 744
user entitlements
about viewing 714
user menu 7-8
user name credential
create using Policy Tree 927
creating 912
user permissions 721, 739
about 713
adding Master admin role 710
user settings 8
user-generated key 581
username and password 764
username credential
creating 913
username password 764
users 746

V

validation 12, 74, 632, 850

VCC

see Venafi Configuration Console 44

vcc 46

Venafi Configuration Console

about 44

venafi configuration console 46

Venafi Operational Certificate 57, 535-536

Venafi Platform 509

Venafi Recycle Bin 138, 143, 145

Venafi service modules

starting or stopping 64

Venafi Trust Protection Platform

configuring 44

Verification Mode 839

view 150

view license 75

VOC

see Venafi Operational Certificate 57, 535-536

W

Web SDK 75, 851

web server 64

WebAdmin

about buttons in the Tree view 22

about the Tree view 19

adding objects 28

deleting objects 31

Detail view 23

Detail view buttons 23

filtering the Tree view 37

logging in 17

moving objects 33

renaming objects 36

Reports tab 19

starting in Query mode 41

Tree view
Add button 22
Delete button 22
Filter button 22
Refresh button 22
WebSDK 75, 851
Widgets 599
Certificate Authorities 600, 615
Certificate Expiration 600, 616
Certificate Key Size 600, 614
Certificate Origin 616
Certificate Protection Level 601, 615
Certificate Signing Algorithm 601, 614
Certificate Totals 602
Certificate Trends 605, 616
Certificate Validity Period 607, 615
Client Certificate Totals 610
Key Size 621
Key Totals 618
Network Discovery–Key Size 622
SSH Key Algorithm 620
SSH Network Discovery Summary 623
SSH trends 627
Trust distribution per User 626
Windows authentication
alternate options 791
for Web consoles 796-797
Windows Registry
enabling Demo Mode 985
Work
setting permissions for 734

X

x-forwarded-for 353, 507