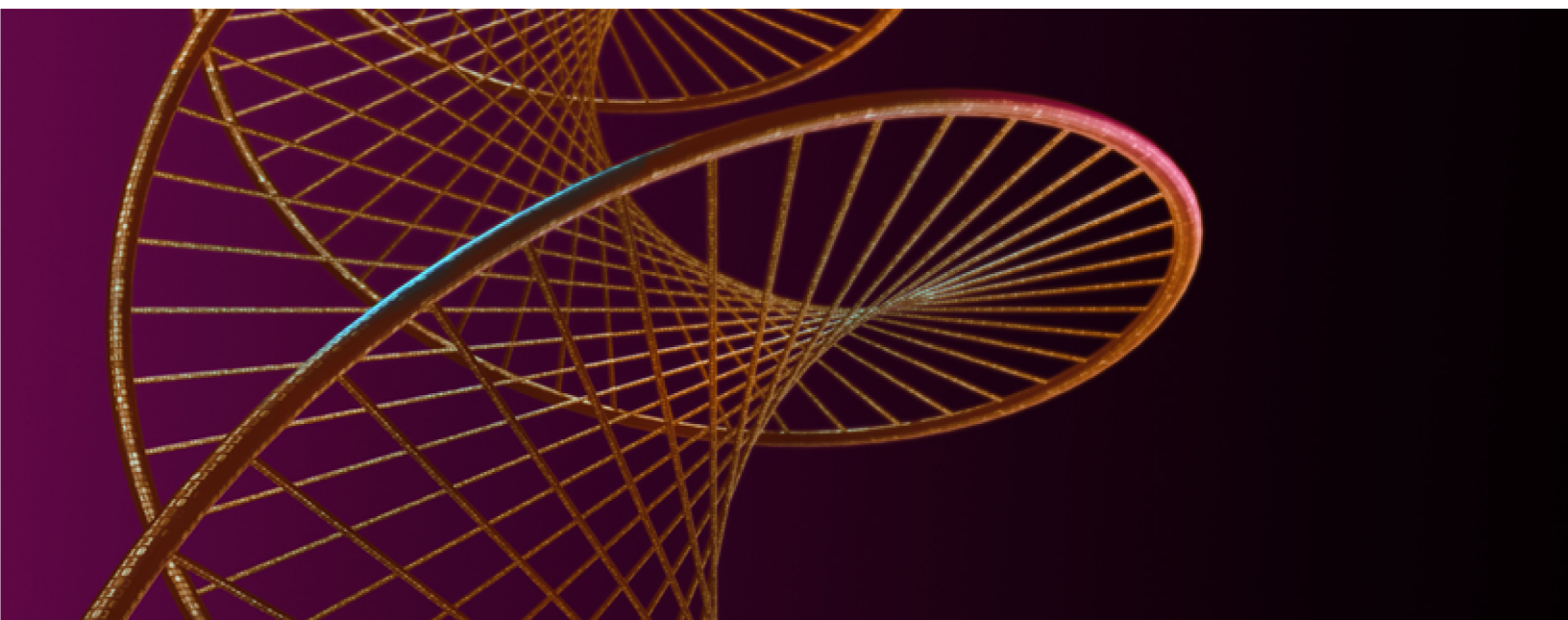


Venafi Trust Protection Platform 25.1

Certificate Management Guide



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 (Certificate Management 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

Venafi TLS Protect Introduction	16
Venafi TLS Protect tasks based on role	17
Audience	18
Documentation Conventions	18
Chapter 1: Managing certificates and keys	19
VIA Venafi and our No Outage Guarantee	20
Managing certificates and private keys—overview	21
Functional overview	22
About Monitoring (Trust Authority)	25
About Enrollment (Trust Authority)	25
Certificate Installation (Provisioning) – Trust Force™	26
Unassigned certificates	27
About certificate lifecycle management	27
Certificate object hierarchy	30
Overview of certificate types	31
Changing a certificate's type	35
About tracking certificate inventory	36
Opening the certificate inventory	37
Certificate status and risks explained	37
Certificate errors explained	43
Changing the management type to Provisioning	44
Viewing the Policy's Certificates	45

Policy object View tab options	46
Creating reports from Policy View tab data	49
Network and local certificate management configuration overview	50
Local certificate management quick start	51
Chapter 2: Discovering certificates and keys	55
Using network discovery	57
Creating a network discovery job	58
Managing the discovery server	61
Configuring discovery zones	62
Excluding IP addresses and host names from discovery scans	63
About network discovery objects	66
Using Onboard Discovery	70
Onboard Discovery prerequisites	70
Creating a new Onboard Discovery job	73
Adaptable Onboard Discovery sample script	80
Using Instant Discovery	83
Using Kubernetes discovery	83
Creating a new Kubernetes Discovery job	84
Organizing discovered certificates and keys	87
Creating placement rules	87
Editing discovery placement rules	90
Editing the order in which placement rules are executed	93
Deleting a network discovery placement rule	94
Assigning permissions to placement rules	94
Certificate and Device Placement jobs	96
Creating Certificate and Device Placement jobs	96
Viewing and editing Certificate and Device Placement jobs	98

Certificate and Device Placement job details	98
About combining duplicate certificates during placement	101
Managing discovery jobs	103
Filtering the Jobs list by job type	104
Scheduling a job	105
Prioritizing network discovery jobs	106
Editing job settings	106
Renaming a job	107
Deleting jobs	108
Running a job manually	109
Manually running, canceling, or pausing a discovery job	110
About placement of duplicate certificates	111
How does TLS Protect determine if a certificate is a duplicate?	112
Moving certificates and keys in bulk after Discovery	112
Enabling a discovery placement engine	115
Specifying discovery exclusion objects	115
Chapter 3: Importing certificates from a certificate authority	117
Importing certificates from an Amazon Private CA	118
First things first	118
Importing certificates from a Microsoft CA	120
Importing certificates using the Adaptable CA driver	123
About automating PowerShell script updates following service URL and configuration changes	126
Using sample Adaptable PowerShell scripts	127
Running a CA import manually	128
CA Import reconciliation rules	129
Verify certificate import results	129

Enable or disable a CA import service module	131
Chapter 4: Managing network certificates and private keys	133
Bringing network certificates under management	135
About importing existing certificates	135
Importing an existing certificate	135
Retrieving certificates	137
Re-import a certificate from a network address	138
Managing certificate configuration	139
Overview of certificate types	139
Configuring the certificate management level	143
Configuring certificate objects	145
About certificate object settings	146
About Subject Alternative Names (SANs)	174
Setting policy on a folder	177
About a certificate's summary (Policy Tree)	185
About Viewing Certificate History	187
Configuring certificate settings via policy	188
Policy object certificate settings	190
Policy object monitoring settings	199
Determining certificate compliance	201
Associating certificates with applications	202
Associating a certificate with an application object	203
Associating a certificate with an application from the certificate object	206
Associating certificates with multiple applications (one-to-many)	211
Extracting certificates and private keys	213
Renewing a certificate manually	214
Manually uploading the CSR	216

Manually Uploading the Private Key	218
About clearing certificate workflow errors	218
Clearing Certificate Workflow Errors	220
About revoking certificates manually	220
Revoking a certificate	223
About Revocation Checking	226
About Certificate Revocation	227
Supported Methods of Revocation Publication	228
Checking the revocation status of certificates	228
Revocation and endpoint reason codes	230
Disabling (or enabling) CDP monitoring and revocation checking	235
Viewing the revocation status of multiple certificates	236
Validating Certificate Revocation Lists - Overview	236
About Supported URL Formats	238
Understanding CRLs and CDPs	238
Enabling CRL Verification	241
Adding CDP Entries	245
Setting the Expiry Notification Percentage	247
Disable a CDP entry or modify a CDP description	248
Configuring CRL notifications and email messages	248
Pushing Certificates and Private Keys to Applications	249
Pushing a certificate and private key to an application	250
Pushing a Certificate and Private Key to an Application from the Certificate Object	250
ACME integration with TLS Protect	251
About the ACME protocol	252
About Venafi Support for ACME v2	252
About using the win-acme client	253

About using the acme.sh client	253
Installing the ACME Service	254
Enabling and configuring ACME using TLS Protect	254
ACME domain challenge	257
About requesting an ACME certificate using certbot	258
Basic ACME certbot commands	259
ACME v2 revoke certificate endpoint	261
Viewing ACME certificates	262
Chapter 5: Certificate enrollment via SCEP protocol	265
Configuring SCEP support on Trust Protection Platform	268
Configuring network device enrollment	269
Network device enrollment settings—Platforms and Server object	277
About Network Device Enrollment rules	283
Using rules to manage SCEP Certificate objects	284
Example of rule execution	286
Using a policy to configure NDE	287
Chapter 6: Managing local certificates	293
About self-signed certificates in Trust Protection Platform	294
Configuring a self-signed certificate template	296
FAQ: Self-signed certificates	299
Configuring certificate objects	302
About local certificate settings	303
About a certificate's summary (Policy Tree)	311
Certificate Status section	312
Associated Applications	313
Certification Path	313
Certificate Details	313

About Viewing Certificate History	313
Revoke historical certificates	314
Revert historical certificates	315
Download historical certificates	316
Managing Local Certificates Via Policy	317
Policy object certificate settings	319
Policy object monitoring settings	327
Using PBE (password-based encryption) algorithms to secure private keys	329
Determining certificate compliance	330
Chapter 7: Managing root certificates	333
Bringing discovered root certificates under management	334
Manually adding root and intermediate root certificates	334
Deleting Root or Intermediate Root Certificates	336
Downloading root chains	336
Blacklisting root or intermediate root certificates from chain building	338
Chapter 8: Managing certificate trust	339
Managing root certificate trust	340
Managing certificate bundle objects	341
Creating a certificate trust bundle	341
Strict matches versus allowable matches	342
Viewing trust bundle associations	345
Viewing the Effective Bundle	346
Creating and managing trust stores	348
About creating and configuring trust stores	350
Configuring a Blue Coat trust store	352
Configuring a CAPI trust store	354

Configuring an IBM DataPower trust store	356
Configuring an IBM Sterling Connect:Direct trust store	359
Configuring an F5 LTM Advanced trust store	362
Configuring a GSK trust store	364
Configuring a JKS trust store	367
Configuring a Palo Alto Networks trust store	369
Configuring a PEM trust store	372
Configuring a PKCS#12 trust store	374
Adding a trust bundle to a trust store	377
Provisioning bundles to trust stores	383
Creating a certificate workflow	383
Enabling regular updates for compliance	389
About Domain Whitelisting	391
Chapter 9: Managing certificate notifications	393
About certificate notification and logging	394
Notification and logging overview	394
Setting up notifications and logging	395
Notification object settings	396
Chapter 10: Working with lost certificates	399
Finding assets using filters on the Certificate Inventory list	400
Filter Panel Groups and Filter Types	400
Find certificates assigned to a specific user	409
Editing columns in the Certificate Inventory list	411
Check for Lost Certificates	417
Taking ownership of a lost certificate	418
About the Aperture configuration object	419
About Identities and Permissions	420

Setting up Identities	420
Assign Permissions to Identities (users and groups)	422
About Notifications	428
Setting up notifications and logging	429
Notification object settings	430
Customizing email notifications	432
Creating notification rules	432
Working with the Rule Editor	434
Account settings for expiring certificates	437
Chapter 11: Working with certificates	439
Creating a new certificate	440
Choosing a key algorithm based on the certificate authority (CA)	443
About RSA and elliptic curve cryptography (ECC) key algorithms	446
Taking action on a certificate	447
View an individual certificate's details, including certificate permissions and installations	448
How long does it take for a certificate authority (CA) to issue a certificate?	451
Downloading certificates, private keys, and root chains	453
Extracting and downloading PEM contents into separate files	457
Configuring validation for certificates	460
Renewing a certificate manually	461
Revoking a certificate	463
Checking revocation status of a certificate	465
Retiring a certificate	465
Reactivating a retired certificate	466
Scheduling a certificate renewal	468
Resolving certificate errors	469

Renaming a certificate	470
Deleting a certificate	471
Moving certificates and keys in bulk after Discovery	472
Working with certificate installations	475
Creating certificate installations (applications)	476
Creating a certificate installation	476
About deleting installations	479
Delete a certificate installation	479
Creating a new user credential for certificate installations	481
Edit the Installation Type	482
Edit a certificate's installation details	483
Approve or reject a workflow ticket for a certificate installation	484
Cancel a certificate installation	484
Retry a certificate installation	485
Replace a certificate installation	485
About adding an installation to a certificate	486
Running validation scans	486
Frequently Asked Questions	487
How certificate renewal works	489
Implications for renewing reverted certificates	490
Sorting certificates in the Policy Tree Certificates grid	490
About Domain Components	491
Controlling domain components by policy	492
Chapter 12: Certificate installation	493
About certificate installation methods: agentless versus agent	496
Configuring devices for certificate installation	498
Setting, editing, or renaming devices and credentials (Agentless)	499

Device object settings (agent and agentless)	500
Using the Server Agent to install certificates	508
Managing applications	509
Editing an application	509
Changing the management type to Provisioning	511
Configure a Certificate Authority to enroll and renew the certificate	512
About workflow objects used during certificate installation	512
Approving or rejecting a certificate installation	512
Configuring certificate workflow approval to receive notifications	513
Installing (provisioning) lots of certificates and keys at one time	514
Before you create and run a new bulk provisioning job	515
Creating a new Bulk Provisioning job	515
Using sample Adaptable Bulk Provisioning PowerShell scripts	518
PowerShell script reference for Adaptable Bulk Provisioning	520
Protecting against unapproved changes to Adaptable Bulk Provisioning scripts	524
Editing an existing bulk provisioning job	525
Scheduling a bulk provisioning job	525
Renaming a bulk provisioning job	526
Running a bulk provisioning job manually	527
Configuring Bulk Provisioning Manager service module settings	528
Viewing Bulk Provisioning log events in Policy Tree	529
Renewing a certificate manually	529
Installation statuses explained	531
Validating a certificate's installation (onboard validation)	533
Validation of a certificate's installation (agentless)	535
Validation of a certificate's installation (Server Agent)	536
Disabling onboard validation	538

Chapter 13: SSL/TLS network validation	541
About configuring validation	544
About configuring validation on the Policy Tree	544
Validation Manager daily scans	544
Server name indication (SNI) support for validation	545
Supported certificate ciphers for network validation	545
Configuring validation for certificates	545
Configuring validation for applications	546
Running validation scans	547
Review validation results	548
Validation Status	548
Disabling SSL/TLS validation	554
Chapter 14: Implementing certificate workflow management	557
About workflows	558
About Workflows in Trust Protection Platform	558
Creating a certificate workflow	560
Workflow object settings	565
Defining reason codes for certificate approvals	573
Applying or blocking application workflows	577
About Adaptable Workflows	578
Adaptable Workflow prerequisites	579
PowerShell script reference for Adaptable Workflow	580
About hash tables for Adaptable Workflow	581
Creating new data fields for Adaptable Workflow	582
Process function	584
Creating an Adaptable Workflow	588
Protecting against unapproved changes to Adaptable Workflow scripts	593

Managing approval requests in the Policy Tree	594
Managing certificate approval requests	596
About approval duration	599
About workflow approvers	601
Viewing pending approvers for a workflow	602

Venafi TLS Protect Introduction

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.

Venafi TLS Protect allows certificate administrators to track certificate usage and compliance in their organization, discovering certificates across the enterprise, and eliminating certificate-caused outages by ensuring certificates are renewed before they expire. Server owners use TLS Protect to see the certificates assigned to them in the system, renew certificates, and take other role-appropriate actions (which might include, for example, creating and managing teams, or approving certificate issuance and renewal via work flows).

If you're already familiar with certificate management and want to find instructions for a task based on your role, use the links below.

Venafi TLS Protect tasks based on role

Role	Suggested Topics
Master Admin	▪ Upgrading to the 25.1 quarterly release ▪ Alternate authentication and login options (including single sign-on) ▪ "Organizing discovered certificates and keys" on page 87 ▪ "Importing certificates from a certificate authority" on page 117 ▪ Configuring the Venafi Trust Protection Platform server object ▪ Using policies to manage encryption assets
Server Owner	▪ "Finding assets using filters on the Certificate Inventory list" on page 400 ▪ "Creating certificate installations (applications)" on page 476 ▪ "View an individual certificate's details, including certificate permissions and installations" on page 448 ▪ "Creating a new certificate" on page 440 ▪ "Renewing a certificate manually" on page 529 ▪ "Scheduling a certificate renewal" on page 468 ▪ "Downloading certificates, private keys, and root chains" on page 453

Role	Suggested Topics	Audience
Certificate Approver	▪ "About workflows" on page 558 ▪ "Managing certificate approval requests" on page 596 ▪ "Viewing pending approvers for a workflow" on page 602	
Team Owner	▪ Working with teams ▪ Creating and managing teams ▪ Editing teams	
API Developer and Dev Ops	▪ Setting up token authentication ▪ Web SDK REST for all products ▪ Auth SDK for token management ▪ Trying out the Web SDK in Swagger ▪ Confirming service status ▪ Getting a certificate signing request enrolled	

Audience

Documentation Conventions

All references to Secure Socket Layer (SSL) in this manual also refer to Transport Layer Security (TLS) unless specifically stated otherwise. In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path. Items that appear in **bold** refer to button, file, directory, icon, and volume names as well as items in lists and menus. Within a command or pathname, items that appear in *italic* refer to a variable. When used in reference to a command, the term “enter” indicates that you should press the Enter key after typing the command.

1

Managing certificates and keys

This section provides a high level overview of certificate and private key management and describes Trust Protection Platform's encryption management services. It also shows you how you can use Trust Protection Platform to ensure that encryption is reliably deployed and managed throughout your encryption environment.

This chapter contains the following topics:

VIA Venafi and our No Outage Guarantee	20
Managing certificates and private keys—overview	21
About tracking certificate inventory	36
Network and local certificate management configuration overview	50

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](#).

Managing certificates and private keys—overview

Venafi Trust Protection Platform™ TLS Protect automates the discovery, monitoring, validation, enrollment and provisioning of encryption keys and digital certificates.

Trust Protection Platform's third-generation architecture supports many certificate authorities (CAs), multiple platform deployments and various encryption types (symmetric, asymmetric and SSH), and has proven scalability within the world's largest enterprises.

This section provides an overview of the certificate management options now available in Venafi Trust Protection Platform. This information provides a conceptual framework that you can use to determine how you want to manage certificates in your own organization.

This chapter contains the following topics:

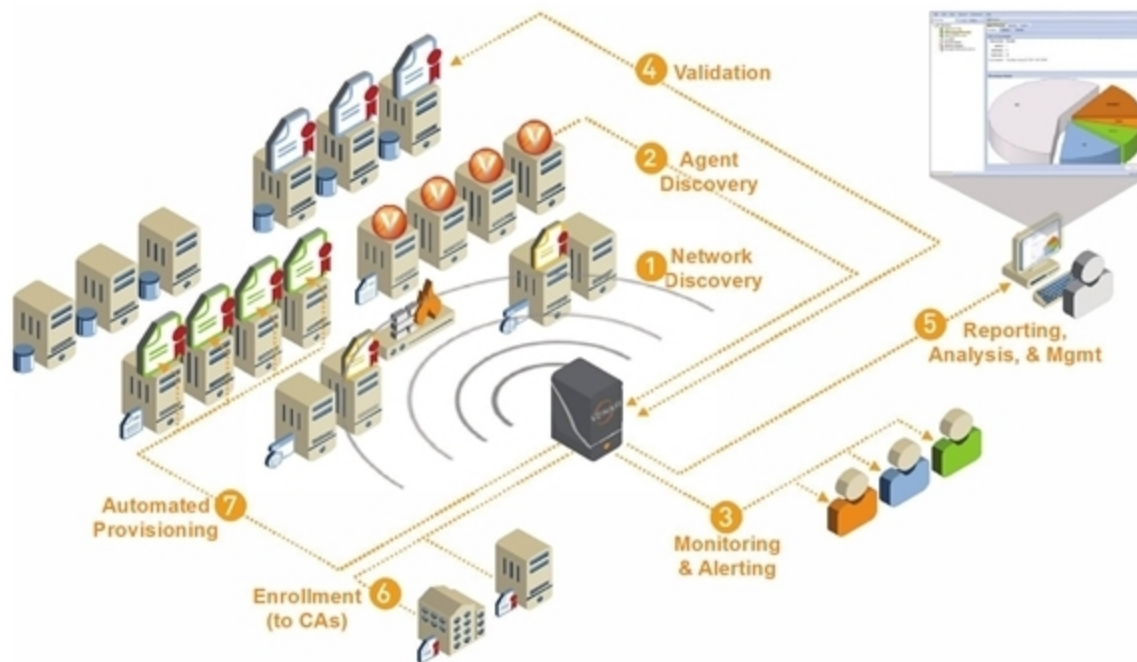
Functional overview

Encryption has become ubiquitous in today's IT infrastructure and is critical in any machine identity management strategy. Digital certificates are a core component of the larger encryption landscape for securing communications and authenticating users and systems for protocols such as SSL and IPSEC.

While certificates and their associated private keys are leveraged heavily for mission-critical applications, they do not come without overhead. First, the trust and validity of a certificate is time limited—typically valid for one year—and must be renewed before the lifecycle period expires or system outages and downtime occur. Second, although the public portion of a certificate is freely transmitted, the private portion must be kept secret and properly managed to avoid data or system compromise. Finally, the certificates and private keys must adhere to current encryption standards and best practices.

Trust Protection Platform enables you to rapidly develop an accurate certificate and key inventory and identify security and operational risks. Additionally, you can quickly evaluate your compliance with corporate and regulatory folders and establish a concise methodology to ensure compliance. With built-in management and policy best practices, Trust Protection Platform helps eliminate data breaches, security audit failures and unplanned system outages.

Trust Protection Platform enables you to quickly quantify your certificate and private key-related risk. Once quantified, it is possible to manage that risk and drastically reduce exposure.



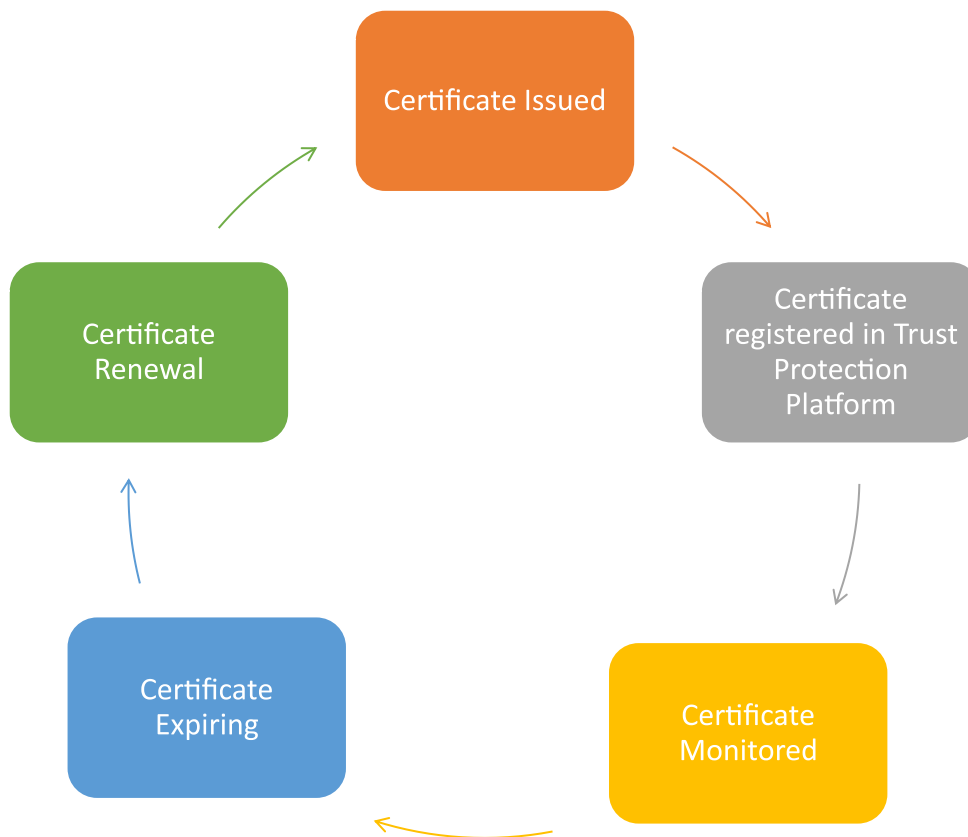
To address the needs of diverse organizations with varied security requirements, Trust Protection Platform provides discovery plus three levels of certificate and key management:

- Monitoring (Trust Authority)
- Enrollment (Trust Authority)
- Provisioning (Trust Force)

Additionally, some items may be in your system, but are not managed by Trust Protection Platform. These items are identified as "Unassigned."

Certificate Lifecycle

It is important to understand the certificate lifecycle, and how Trust Protection Platform manages each stage of the certificate lifecycle.



Certificate issued

Certificates are issued by a Certificate Authority (CA).

Certificate registered in Trust Protection Platform

When you first start using Trust Protection Platform, these certificates are not known to the system, and you need to get the certificates registered in the system so you can manage them effectively. Once certificates are being managed in Trust Protection Platform, the system can be configured to issue and deploy these certificates automatically, or you can do this manually, depending on your organizations policies and procedures.

Certificates are registered in Trust Protection Platform in one of two ways:

- **Discovery:** Certificates are discovered on your devices, or are imported into Trust Protection Platform directly.
- **New Requests:** There are three ways new requests can work in Trust Protection Platform
 - *User provided CSR.* In this case, you create the certificate signing request (CSR), and provide the private key. You import the CSR into Trust Protection Platform, and Trust Protection Platform submits the CSR to the CA.
 - *System generated CSR.* In this case, Trust Protection Platform generates the CSR and the private key, and stores the private key in the Secret Store. Trust Protection Platform submits the CSR to the CA.
 - *Remote Key generation (Provisioning-level only).* In this case, Trust Protection Platform connects to the system where the certificate will be deployed, and that machine generates the CSR and private key, and stores the private key locally. Trust Protection Platform then submits the CSR to the CA.

Certificate monitored

During this phase of a certificate's lifecycle, the certificate is being constantly monitored to ensure the certificate is being used correctly in your system, and alerting you to any issues or errors found that are related to this certificate.

Certificate expiring

When the certificate is close to expiring, Trust Protection Platform notifies and allows- you to decide if you want to renew the certificate or not. You can create policies that allow certificates to automatically renew or not, based on your preferences, and the type of certificate being managed.

Certificate renewal/EOL

If you choose to renew a certificate, you can use Trust Protection Platform to create the renewal request, or you can create the request yourself and import it into Trust Protection Platform. If a certificate has reached the end of its lifecycle and doesn't need to be renewed, you can revoke or retire the certificate to ensure it is no longer used in production systems.

If you have questions about how this process works, we recommend talking to your system administrator.

About Monitoring (Trust Authority)

At this level of management, organizations can continuously monitor key and certificate assets for improved inventory and risk mitigation. Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform sends dynamically-generated expiration and escalation messages to certificate owners, consumers, and approvers.

At the monitoring level of certificate management, however, Trust Protection Platform does not renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then retrieve and install the renewed certificate.

Once the certificate is manually installed, Trust Protection Platform can validate the certificate is installed and properly configured.

Monitoring is available for both network and local certificates. Monitoring is enabled in the Certificate object configuration. For more information, see ["Managing certificate configuration" on page 139](#).

To learn how to change a certificate's management type, see ["About certificate object settings" on page 146](#).

About Enrollment (Trust Authority)

At this level, Trust Protection Platform interfaces directly with Certificate Authorities (CAs) to initiate and auto-enroll new or to-be-renewed certificate and key generation requests according to organization-defined workflow and approved folders.

Trust Protection Platform automatically generates and submits CSRs to CAs using the parameters defined in designated CA Template objects. If preferred, administrators can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA.

Trust Protection Platform can renew external certificates through integration with several supported external CAs using existing or new private keys. In each case, the term of the renewed certificate is extended to include any life remaining on the previous certificate.

NOTE This feature is not provided for internal CAs only because it does not make sense to extend days on an internal certificate.

After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the Secret Store. The administrator can then download the certificate from the Secret Store and install it on the target system(s).

Enrollment is available only for network SSL certificates. Enrollment is enabled in the Certificate object configuration. For more information, see ["Managing certificate configuration" on page 139](#).

For an explanation of the managed stages of the certificate lifecycle, see ["About certificate lifecycle management" on the facing page](#).

To learn how to change a certificate's management type, see ["About certificate object settings" on page 146](#).

Network Device Enrollment

In addition to conventional certificate enrollment, Trust Protection Platform now supports certificate enrollment via 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 on Network Device Enrollment, see ["Certificate enrollment via SCEP protocol" on page 265](#).

Certificate Installation (Provisioning) – Trust Force™

Venafi TLS Protect provides a fully automated certificate and key life-cycle management, one that **automatically requests, installs, renews, and monitors encryption assets on your network**. This produces consistent and repeatable processes that improve security and reduce operational and compliance risks.

To learn more, see ["Certificate installation"](#) on page 493 in the *Trust Protection Platform Certificate Management Guide*.

Unassigned certificates

Unassigned certificates are unlicensed Trust Protection Platform certificates that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.

To learn how to change a certificate's management type, see ["Changing a certificate's type"](#) on page 35 in the *Trust Protection Platform Certificate Management Guide*.

About certificate lifecycle management

Trust Protection Platform simplifies the process of managing digital certificates throughout their lifecycle. When a certificate is brought under management, Trust Protection Platform monitors the certificate and provides current information about the certificate status. When a certificate nears the end of its lifecycle, Trust Protection Platform provides notifications so you can renew and install the certificate before it expires.

If a network certificate is configured for Enrollment, Trust Protection Platform interfaces directly with the CA to initiate certificate renewal and key generation requests according to organization-defined workflow and approved folders. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the Secret Store. The administrator can then download the certificate from the Secret Store and install it on the target system(s).

If a network certificate is configured for Provisioning, Trust Protection Platform automatically requests, renews, and installs the certificate on its associated application(s), ensuring that the certificate is reliably deployed and managed.

NOTE Individual stages may vary per application. For information on the certificate lifecycle stages for each application, see [Managing Applications](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

The following table outlines the managed stages of the network certificate lifecycle.

Certificate enrollment involves two distinct "todo" items. The Certificate ToDo (stages 0-450), and Certificate Enrollment ToDo (stages 500-750). These ToDos respect different engine assignments. For example, the Certificate ToDo respects what is specified for the certificate object, but the Certificate

Enrollment ToDo respects what is specified on the CA Template. If you are seeing certificate processing failures (including while using Intune), try setting the engine assignment to be the same on both the certificate object and the CA template.

NOTE If the private key and CSR are locally generated on the Trust Protection Platform server, stages 0-700 are performed by the default X509 Certificate Application driver. Stages 0-700 are only performed by the certificate's consumer Application driver if the private key and CSR are remotely generated on the certificate's consumer application.

The private key and CSR are remotely generated on the certificate's consumer applications if the **Generate Key/CSR on Application** option is enabled in the Certificate object.

Stage Codes and Descriptions

Certificate Stage Codes

Stage Code	Friendly Name	Description
0	StartProcessing	Prepares the certificate for lifecycle processing.
100	CheckStore	Applies only to remote generations. If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.
200	CreateConfigureStore	Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object.
300	CreateKey	Creates the private key. DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400.

Stage Code	Friendly Name	Description
400	CreateCSR	Creates the Certificate Signing Request (CSR). If Service Generated CSR is enabled and the certificate is associated with multiple applications, the CSR will be centrally generated so Trust Protection Platform can push the private key to multiple applications.
500	PostCSR	Submits the CSR to the Certificate Authority (CA). If you post a manual CSR, this is the first stage of the certificate lifecycle.
600	ApproveRequest	Approves the certificate renewal at the CA.
700	RetrieveCertificate	Retrieves the certificate from the CA.
800	InstallCertificate	Installs the certificate on the target application. This provisioning happens in several stages, such as 801, 802, etc. All stages between 800-899 are provisioning stages.
900	CheckConfiguration	Reserved for future use. You cannot apply this stage to a workflow.
1000	ConfigureApplication	Reserved for future use. You cannot apply a stage to this workflow.
1100	RestartApplication	Used for command injection workflow that must be executed after a certificate has been successfully provisioned.
1200	EndProcessing	Completes the certificate processing and, if configured, runs a Validation check on the certificate and application.

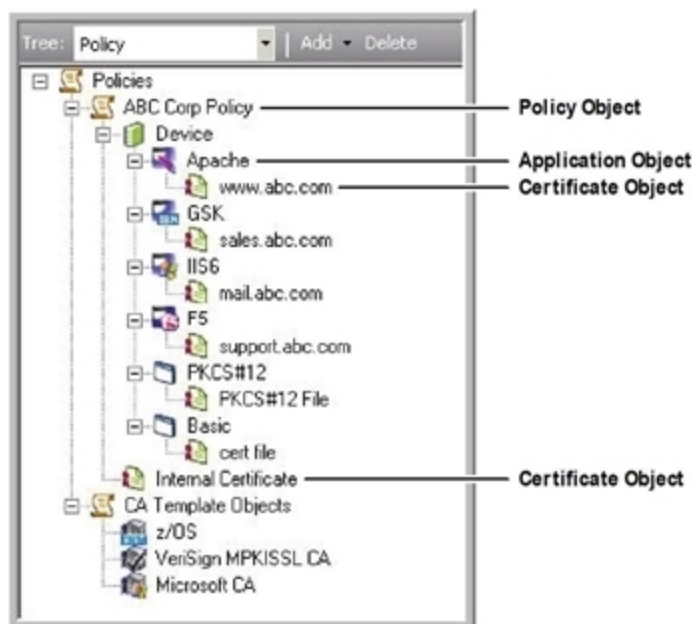
Stage Code	Friendly Name	Description
1400	Revocation	Submits a revocation request to the CA. Certificate revocation is a certificate operation; it does not involve the application driver.
1500	UpdateTrustStore	Updates the Trust Store at the host to comply with the effective bundle. To learn more, see "Viewing the Effective Bundle" on page 346 .
1600	EndTrustStoreProcessing	Completes the processing of the Trust Store.

Certificate object hierarchy

Certificate objects are managed in the Policy tree. To access the Policy tree, from the TLS Protect menu, click Policy Tree .

The Policy tree provides a hierarchical view of your encryption deployment model, so Certificate objects appear in context of other system objects such as Policy, Device, and Application objects.

In the Policy tree hierarchy, Certificate objects can be created under Policy or Application objects.



SSL certificates brought under management via Network Discovery are often located below their associated Application object. If you do not create a Network Certificate object below its associated Application object, Trust Protection Platform displays a Certificate Alias object below the associated Application object so you can see which certificates are associated with which applications.

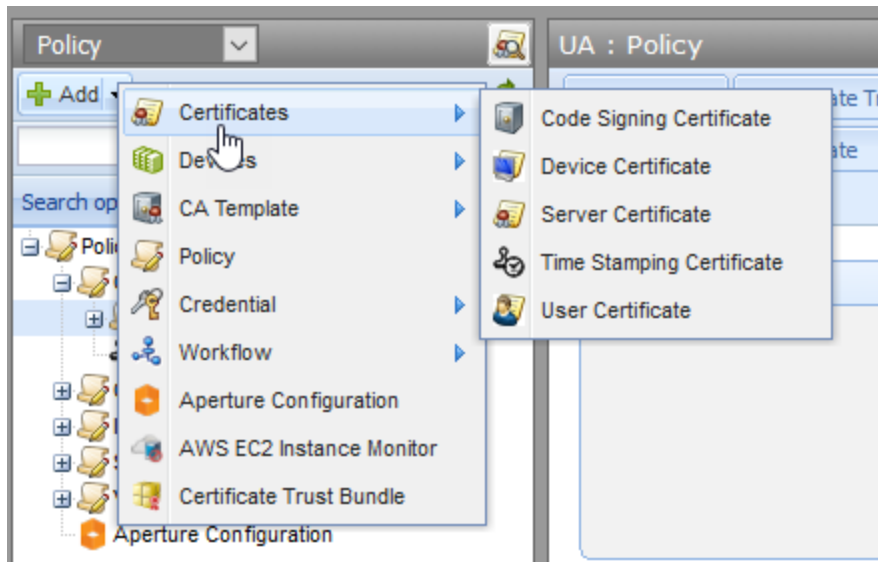
NOTE Alias objects are hidden by default. To view Alias objects in the Policy tree, you must enable the **Show Aliases** option. In the Windows console, click **File > Preferences > Policy Tree**, then select **Show Aliases**. In Policy Tree, click **Show All > Show Aliases**. For information on manually associating certificates with Application objects, see "[Associating certificates with applications](#)" on page 202.

Local certificates brought under management via Agent Discovery are typically created under folder since they may reside on workstations rather than servers and they are managed only under Monitoring, so an associated application configuration is not required.

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 the key should be stored.

What will the different certificates look like?

A certificate type displayed in TLS Protect:

Home / Certificates / AShore-Client

AShore-Client

Download

Client Device Certificate

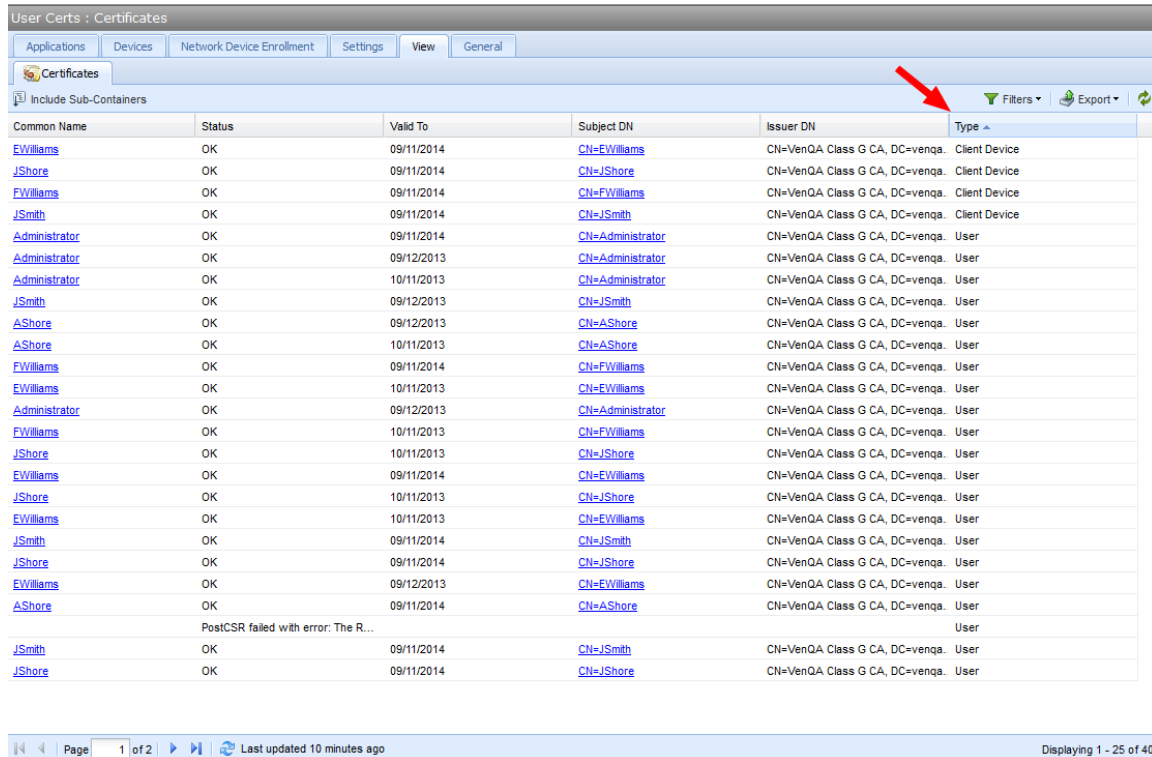
Issuer	Common Name	Organization	Organizational Unit	Locality	State / Province	Key Size
Self Signed	ashore@venqa.venafi.com	Venafi Inc.	Development	Salt Lake City	Utah	1024
Key Usage		Enhanced Key Usage				
Digital Signature, Key Encipherment (a0)		Client Authentication (1.3.6.1.5.5.7.3.2)				

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.

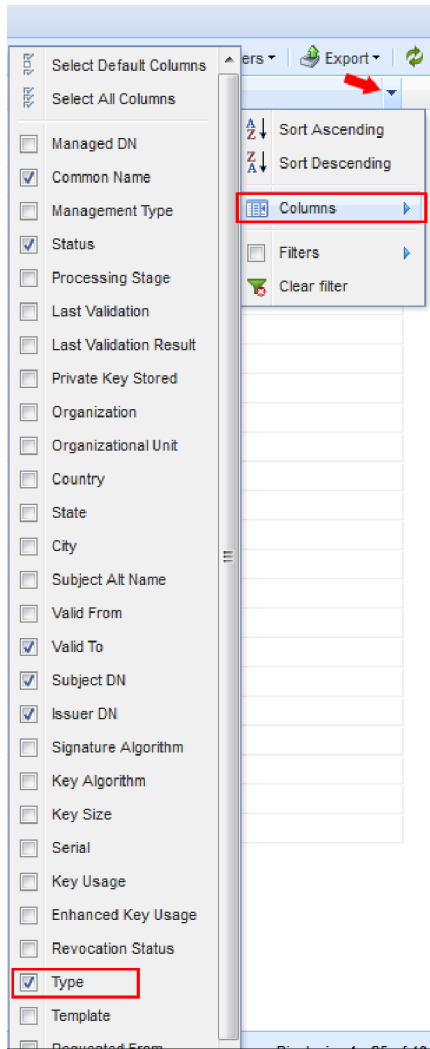


The screenshot shows the 'User Certs : Certificates' window with the 'View' tab selected. A red arrow points to the 'Type' column header in the grid. The grid contains 25 rows of certificate data.

Common Name	Status	Valid To	Subject DN	Issuer DN	Type
EWilliams	OK	09/11/2014	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	Client Device
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	Client Device
FWilliams	OK	09/11/2014	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	Client Device
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	Client Device
Administrator	OK	09/11/2014	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	09/12/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	10/11/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
JSmith	OK	09/12/2013	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	09/12/2013	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	10/11/2013	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
FWilliams	OK	09/11/2014	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	10/11/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	09/12/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
FWilliams	OK	10/11/2013	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	10/11/2013	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	09/11/2014	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	10/11/2013	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	10/11/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	09/12/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	09/11/2014	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
	PostCSR failed with error: The R...				User
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User

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**.



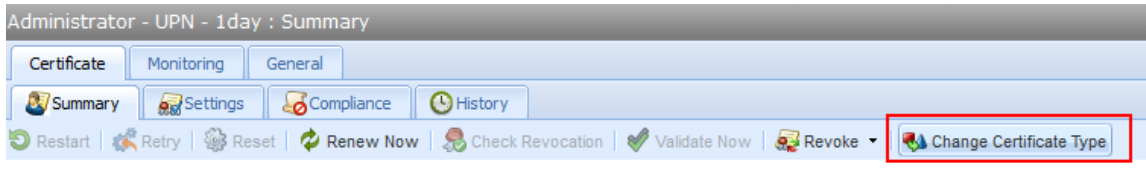
Changing a certificate's type

If a certificate has been misclassified, you can correct it by changing its type. However, use caution when doing so. The certificate's historical data may be lost.

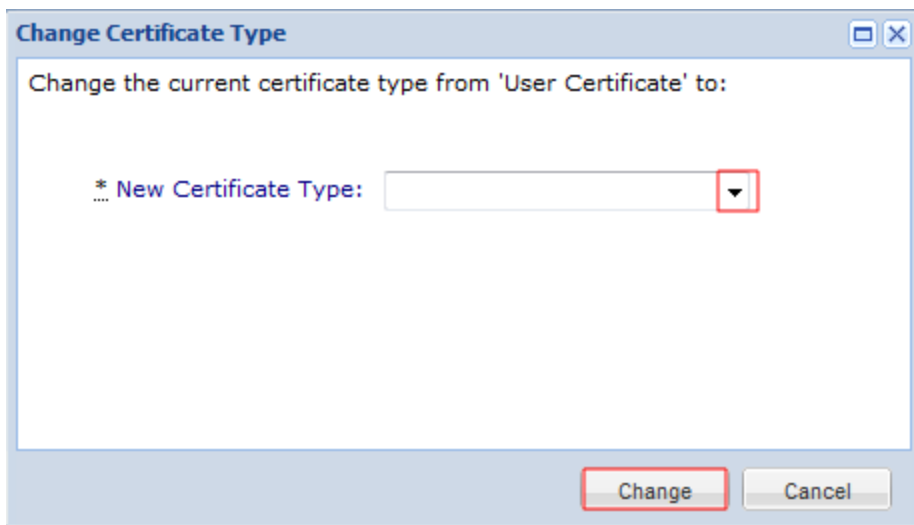
To change a certificate's type

IMPORTANT You must have the *Write*, *Create*, and *Delete* permissions in order to complete this task. You must be logged in to Policy Tree.

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. Find the certificate whose type you want to change, then double-click to open it.
3. Click **Change Certificate Type**.



4. Choose a new certificate type then click **Change**.



To learn about certificate types, see "Overview of certificate types" on page 139

About tracking certificate inventory

Venafi Trust Protection Platform™ provides several ways to track your certificate inventory. You can view an immediate snapshot of your current system in the management console Dashboard, or review all certificates to which you have permissions in the Policy object's Certificates View tab. The Expiration report provides a listing of all certificates that will be expiring within designated time frames.

This chapter contains the following topics:

Opening the certificate inventory

Venafi Trust Protection Platform™ provides several ways to track managed certificates. You can see a list of all certificates and keys to which your user has View permissions. You can see certificate and key details, along with installations, SSL/TLS information, permission information, and the ability to take actions on items in the inventory.

To open Certificate Inventory in Aperture

1. From the Aperture menu bar, click **Inventory > Certificates**.
2. The certificate inventory view opens. Filters are displayed on the left. No certificates are displayed until *after* you enter filter criteria, then click **Apply Filters**.

Certificate status and risks explained

When reviewing the certificate inventory, the inventory list contains several columns including **Status** and **Risks**. The **Status** column shows the most important status of the certificate in the certificate lifecycle. The **Risks** column shows relevant security risks that apply to the certificate.

The two-column format highlights the most important information, the status of the certificate, while still showing the security risks for a given certificate. Both the **Status** and **Risks** columns are visible columns by default.

When the certificate renewal process is stalled for some reason, click the information icon to see specific information about the status, providing you with additional context on what actions need to be taken to resolve the issue. Additional status information is available on the certificate overview page.

List of Statuses

The following table lists the status identified for certificates, along with a brief definition of what the status means.

Since the **Status** column only displays one status at a time, and since a certificate could potentially have more than one of the status items identified, the table includes a **Display Priority** column to show which status will be shown in the **Status** column. If more than one status applies, the status item with the lowest display priority number will be shown.

Status	Display Priority	What It Means	Notes
Disabled	1	Certificates that are retired. They are not included in the dashboard statistics, in-product reports, or licensing of the product. These certificates <i>will be</i> displayed on custom reports.	
Management Type Unassigned	2	A management type that can be given to certificates so that they can be reported on the dashboard but are unlicensed. Typically used during network certificate discovery when placement rules could not place certificates. Unassigned can be used temporarily until certificates can be properly classified.	
Failed Revocation	3	Certificate revocation for the current certificate was attempted but failed and produced an error. Revocations are performed for security reasons. It is important to know when the process fails.	The application will not try again without user intervention. The user must click Retry .
In Error	4	The certificate encountered an error during initial enrollment or renewal, or there are some applications are in error.	This state contains an information icon providing additional information about the error.
Pending My Approval	5	Any certificates that require the approval of the user who is currently logged in. Includes certificates that are currently being renewed, provisioned, or revoked. Historical certificates being revoked will not show up. These requests and the approvals can currently only be done in Policy Tree. For more information on revoking historical certificates, see "About revoking certificates manually" on page 220.	This state contains an information icon with additional information.

Status	Display Priority	What It Means	Notes
Approval Scheduled	6	A workflow associated with the certificate (or application) was approved and scheduled.	
Pending Someone Else's Approval	7	Indicates that the processing of the certificate cannot proceed until some other Trust Protection Platform user approves the required action.	This state contains an information icon with additional information.
Awaiting CSR	8	The renewal of the certificate cannot proceed until a User Provided CSR is uploaded to the certificate	
Pending Revocation	9	The revocation of the certificate is either queued or in process.	
Installing	10	The certificate is currently being installed.	
Renewing	11	The certificate is either being enrolled with a Certificate Authority for the first time or is being renewed.	
Revoked	12	The certificate has been revoked through the Certificate Authority.	
Expired- Long Term	13	The certificate has been expired for an extended period of time. <i>Long Term Expired</i> are certificates that there are no plans to renew, but will be retired instead.	The value for <i>Expired-Long Term</i> is configurable per user. Each user can set his or her own value.
Expired- Short Term	14	The certificate has recently expired. <i>Short term</i> is important because it may contain certificates that have expired but with the intent to renew them.	The value for <i>Expired-Short Term</i> is configurable per user. Each user can set his or her own value. The calculation is the difference between the expiration date and the <i>Expired-Long Term</i> value.

Status	Display Priority	What It Means	Notes
Expiring Soon	15	Certificates that are going to expire soon. Allows the renewal process and necessary workflow approvals to take place before the certificate expires.	The value for <i>Expiring Soon</i> is configurable per user. Each user can set his or her own value.
Not Disabled	16	View all certificates (even Lost certificates) but filter out any certificate that is considered Disabled/Retired.	
Managed	17	Certificates that are <i>Not Lost</i> and <i>Not Disabled</i> . This is the default filter that is applied on the Certificate Inventory page.	NOTE These status items are not displayed in the Status column, however, they are visible if you filter on these values for Status.
Issued	18	(This status is only visible when the specific filter is selected.) Certificates that have completed enrollment and have an issued certificate associated.	

List of Risks

The following table lists the security risks identified for certificates, along with a brief definition of what the risk means.

Risk	What It Means	Notes
Distrusted Entrust	The certificate was issued by one of the following CAs: ▪ Entrust ▪ AffirmTrust These certificates are flagged in some web browsers as being a potential security risk.	When users of these browsers visit a site with one of these certificates, a security warning is displayed in the browser window. If a web site is protected by a certificate from one of these Certificate Authorities (CAs), you may want to have a new certificate issued from a different CA so people (who are using the selected web browsers) won't see the certificate warning when they visit your site.
Failed Validation	Network Validation was attempted but failed. Applies only to certificates, not devices or applications.	Network Validation can be turned on or off. If it's on, the system will try to validate the certificate once a day, whether the previous validation succeeded or failed.

Risk	What It Means	Notes
Invalid Domain Name	The domain name does not match any of the Allowed Domains as defined in the Domain Whitelist. See the certificate's settings.	
Local Dual Control Needed	In order to meet some audit requirements, certificates need to have more than one person overseeing the processing of certificates. This means that there should be at least one Approval Workflow assigned to the certificate. This field allows Venafi Administrators to find certificates that have this security/audit risk so that dual control can be applied.	This status was added to give customers visibility into SANS CSC 17-14, and PCI-DSS. For information on SANS CSC 17-14: https://www.sans.org/critical-security-controls/control/17 . In Trust Protection Platform, every certificate renewal should have an approver. Those certificates that do not have an approver assigned are given this status.
Lost	Certificates that have been discovered through various means but are not claimed. Responsibility for the certificate(s) has not been assigned to anyone.	Certificates that are <i>Lost and Found</i> or Lost are certificates that are located in a directory that has been designated as a lost and found directory.
No Owner Assigned	The certificate uses the default owner because the Contact or Approver is empty, or it is assigned to a local admin account.	Having a correct owner assigned to a certificate is important for several reasons including notifications for expiration or problems that occur during certificate renewal. Tracking who is responsible for a certificate ensures compliance with the following standards: ■ SANS CSC 1704 ■ PCI-DSS
No Provisioning Targets	The certificate is configured for provisioning, but no installations have been configured. As a result, the certificate cannot be provisioned (installed on a device). If this risk is not mitigated, it could result in an outage since TLS Protect can't automatically provision a new certificate before the old one expires.	To resolve, do one of the following: ■ Create an installation (called application in Policy Tree) of any non-basic type, and then associate it with the certificate. ■ Change the certificate from <code>Provisioning</code> to another type;

Risk	What It Means	Notes
	NOTE In Aperture, this risk is shown if there are no installations of any type. In Policy Tree, a similar risk appears if there are no <i>provisioning</i> applications. For example, if you only have a basic installation for a certificate, Aperture will not show a risk. Policy Tree <i>will</i> show a risk, since a basic application cannot be used for provisioning.	
Unapproved Issuer	The certificate issuer is not marked as approved for issuance.	You can either reissue the certificate with a CA that is approved for issuance or you need to add the issuer of the certificate in question to the list of CAs that are approved for issuance.
Unique Name Violation	The certificate's policy does not allow duplicate Common or Subject Alternative Names (SANs).	
Unsafe Validity Period	The certificate's validity period is longer than what is considered safe by PKI cryptographic standards.	This is configurable via the Certificate Account Preferences. See Certificate Account Preferences.
Validation Disabled	Certificate validation is disabled.	

Risk	What It Means	Notes
Weak Key	The certificate key length is considered weak by PKI cryptographic standards.	This is configurable via the Certificate Account Preferences. See Certificate Account Preferences.
Weak Signing Algorithm	The certificate signing algorithm is considered weak by PKI cryptographic standards.	This is configurable via the Certificate Account Preferences. See Certificate Account Preferences.
Wildcard Prohibited	The certificate's policy prevents the use of wildcard characters in the certificate's Common Name.	If a certificate request contains a wildcard, but the policy doesn't allow for wildcards, when you try to renew the certificate, you will see this risk. To mitigate, modify the certificate request to not include a wildcard, or modify the policy to allow wildcards.

Certificate errors explained

When the system is processing certificates (either installing, provisioning, or renewing) errors can sometimes occur. This topic explains the errors you may encounter, and how to locate certificates that are in an error state.

Error types

There are three types of errors that happen during certificate processing:

- **Enrollment Error.** This error happens when a certificate can't be enrolled. This is often due to issues like server connectivity.
- **Installation Error.** This error happens when a certificate that was previously enrolled is now attempting to be installed on a device or application.
- **Renewal Error.** This error happens when you attempt to renew a certificate, but the renewal was unsuccessful. This can also happen due to issues like server connectivity.

Certificate error messages

When a certificate is in an errored state, you can see this in several places in Aperture, including:

- **Certificate Inventory list.** Certificates that are in an error state will show information about the error in the **Status** column.

To filter the Certificate Inventory list to only show certificates in an error state, use the following procedure:

- In the **Common Filters** group, click in the **Status** field, and select the option **In Error**.

The inventory list will automatically update to only show certificates in an errored state.

- **Certificate details page.** Certificates that have errored during the processing phase will have a red error banner at the top of the Certificate overview page. The banner will explain the error type, and give you specific details about the error message. These details can also be seen in Policy Tree, in the Certificate Status panel.

To filter the certificates list in Policy Tree to only show certificates with errors, use the following procedure:

- In Policy Tree, open the **Certificate Dashboard**, and click the **In Error** tab.

Changing the management type to Provisioning

You can change the Management Type of a certificate in two different ways. If the certificate's settings are locked at the policy level, then you must edit the policy.

IMPORTANT You must have the **View** and **Write** permissions in order to make changes.

To edit an individual certificate's management type

1. To learn about management types, see ["Functional overview"](#) on page 22.
2. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
3. Using **Filters** or **Search**, find the certificate you want to edit.
4. Click the certificate's name.
5. In the certificate's details window, click **Renewal Details**.
6. Click **Edit**.
7. (Conditional) If the management type isn't locked at the policy level, then you can change the **Management Type**.
8. When you're done, click **Next**.
9. Click **Close**.

To edit a management type at the policy level

1. From the [TLS Protect menu bar](#), click **Configuration > Folders**.
2. From the list, click the folder (policy) you want to edit.
3. In the sidebar, click **Certificate Policy**.
4. Under **General Settings**, change the **Management Type**.
5. Click **Save**.

To learn about certificate object settings, see "[About certificate object settings](#)" on page 146.

Viewing the Policy's Certificates

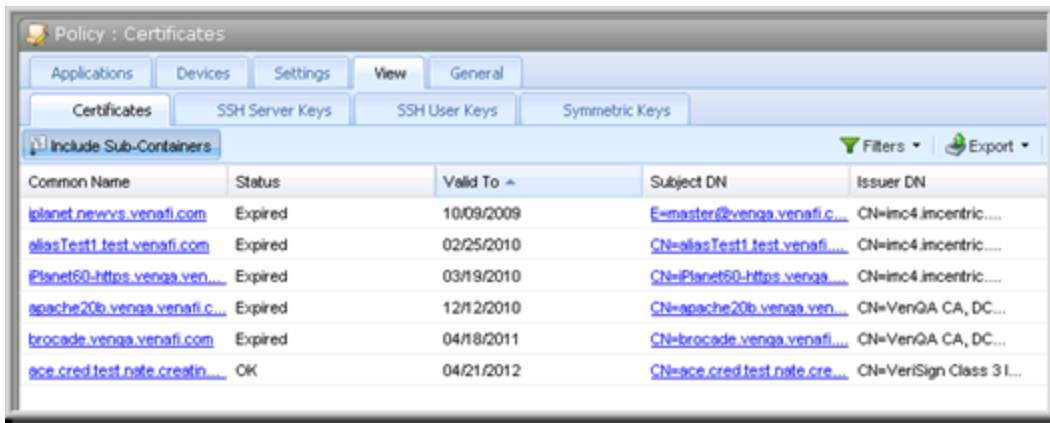
If you distribute certificate management by Policy object, the Certificates View list provides an easy way for individual administrators to view the certificates for which they are responsible because administrators can view only those objects to which they have View permissions.

To view the Policy object's subordinate certificates

1. From the [TLS Protect menu bar](#), click Policy Tree.

NOTE To view the Certificates View tab, you must have Read permissions to the Policy object as well as the subordinate Certificate objects.

2. In the Policy tree, select the Policy object containing the Certificate objects you want to view.
To view all Certificate objects to which you have *View* permissions, select the **Root Policy** object.
3. Click **View > Certificates**.
4. (Conditional) If the current Policy object contains subordinate folder, click **Include Sub-folders** to view all Certificate objects from this point down in the Policy tree.
5. (Conditional) In Policy Tree, click **Load** to populate the View tab.
Policy Tree automatically populates the View tab.
6. The Detail View displays the Policy object's subordinate Certificate objects.



7. (Optional) You can click-and-drag the column borders to resize a column, sort any of the columns in ascending or descending order by clicking the column heading, or filter certificates by criteria you define for a given column. For more information on the options in the Policy object View tab, see "Policy object View tab options" below.
8. (Optional) You can export the certificates listed in the Policy View tab to create your own reports. For more information, see "Creating reports from Policy View tab data" on page 49.

Policy object View tab options

The following table defines the options available on the Policy object's **View** tab.

Option	Description
View Tab	The Policy object's View tabs list the policy's subordinate Certificate object.
Column Sort	To sort the Certificate list by a particular column, click on the column heading. The sort toggles between ascending and descending order. In Policy Tree, the column sort order is stored in the administrator's User object. Therefore, Policy Tree always reflects the user's most recent column sort order, even if the administrator logs in from another workstation. In Policy Tree, the column sort order is reset every time you log in unless you bookmark the page. When you bookmark the page, the column sort order is saved and applied the next time you open that view. To bookmark the page, define the column sort order, and then click the Bookmark option  in the Admin menu.

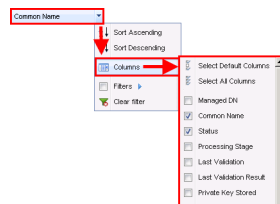
Option	Description
Columns	Determines the columns that display on the View tab. In Policy Tree, the column settings are stored in the administrator's User object. Therefore, Policy Tree always reflects the user's most recent column settings, even if the administrator logs in from another workstation. In Policy Tree, the column settings are reset every time you log in.

To access the Column menu in the Policy Tree

Click the drop-down menu icon for a given column.

Click **Columns**.

From the Columns menu, you can select the columns that you want to display in the View tab.



To access the Column menu in Policy Tree, right-click any column heading, then select the columns that you want to display in the View tab.

If you add the **Template** column, the table cell will be empty unless the certificate has an OID template extension.



Filters

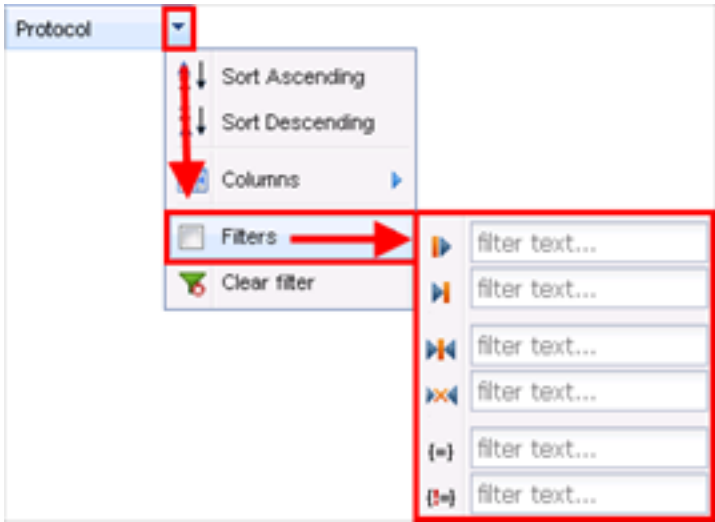
The **Filters** option is available in Policy Tree only. When you define a filter in Policy Tree, the filter is active for the current session only unless you bookmark the page. When you bookmark the page, the filter is saved and applied the next time you open that view. To bookmark the page, define the filter then click the share icon.

Filters the certificates listed in the View tab based on parameters defined for one or more column headings. For example, you can filter the tab to show only Symantec certificates.

To access the Filters menu in the Policy Tree

Option	Description

Click the drop-down menu icon for a given column, and then click **Filters**.



From the **Filters** menu, you can define the criteria by which to filter the current column.

The options in the **Filters** menu depend upon the column you select. For example, in the above example, you can enter a text string to search for a specific key size.

The options in the Filters menu depend upon the column you select.

The following list provides a brief explanation of the text filter icons:

Greater than



Less than



Begins with



Ends with



Option	Description
Contains	
Does not contain	
Equals	
Does not equal	
 Export	Exports the results to a CSV, tab-delimited, HTML, or XML file.
 Refresh	Refreshes the contents of the current page.

Creating reports from Policy View tab data

The Policy View tab provides a listing of the policy's subordinate certificates and their associated data. This data can be very valuable, particularly at the root level of the Policy tree. The Root Policy object lists all Certificate objects in the tree to which you have permissions.

IMPORTANT To view the Certificates View tab, you must have the *Read* permission to the Policy object as well as the subordinate Certificate objects.

The master administrator account has permissions to all objects in the tree and, consequently, can view all objects in the Root Policy View tab.

To create new reports from the folder view tab

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 Policy object containing the Certificate objects you want to view.

4. To view all Certificate objects to which you have View permissions, select the **Root Policy** object.
5. Click **View > Certificates**.
6. Click **Include Sub-folders** to view all Certificate objects in subordinate folder.
7. (Conditional) In Policy Tree, click **Load** to populate the **View** tab.
8. Click **Export**, then export the data to a CSV file.
9. Open the CSV file in a spreadsheet program.
10. [Optional] Use the data to create a pivot report.

Network and local certificate management configuration overview

Trust Protection Platform can manage both network and local X.509 certificates. Using Network Discovery, administrators can identify their network's functional SSL certificates (the certificate must respond to a network SSL query) and bring those certificates under management. Trust Protection Platform can manage network SSL certificates at the Monitoring, Enrollment, or Provisioning levels of certificate management.

Using Agent Discovery, administrators can discover X.509 certificates in local file systems and keystores, then bring them under management for Monitoring. When a local certificate is brought under management, Trust Protection Platform monitors the certificate and provides current information on the certificate status. When a certificate nears the end of its lifecycle, Trust Protection Platform provides notifications so you can manually renew and install the certificate before it expires.

The difference between network and Agent Discovery is that Network Discovery can only discover certificates that respond to SSL queries on designated IP addresses and ports, whereas the Trust Protection Platform Agent can discover certificates located in the file system or keystores.

The following sections outline the steps required to enable both network and local certificate management in Trust Protection Platform:

This chapter contains the following topics:

Local certificate management quick start

The Server Agent discovery feature provides an easy and convenient way to find out what certificates are installed on your local systems. The agent scans the designated directories and keystores, then uploads the discovered certificates to the Trust Protection Platform server.

The difference between network and agent discovery is that Network Discovery can only discover certificates that respond to SSL queries on designated IP addresses and ports, whereas the Server Agent can discover certificates located in the file system or keystores.

To configure the Server Agent to discover certificates in local file systems or keystores, you must first install the agent on the local machine, and then configure the agent's certificate discovery parameters.

Quick Start Checklist for Local Certificate Management

Use the following checklist to help you complete the configuration. You can find an overview of each item in the next section, "[Quick Start Configuration Overview for Local Certificate Management](#)" below.

- Configure the Agent's certificate discovery settings. For more information, see "[Configure the Trust Protection Platform Agent's certificate discovery settings.](#)" on the next page.
- Install the Trust Protection Platform Agent on the machines where you want to discover certificates in the local file system or keystores. For more information, see "[Install the Trust Protection Platform Agent on the machines where you want to discover certificates in the local file system or keystores.](#)" on the next page.
- Configure your certificate expiration Notification Rules. For more information, see "[Configure your certificate expiration Notification Rules.](#)" on page 53.
- Configure and generate the Expiration report. For more information, see "[Configure and generate the Expiration report.](#)" on page 53
- Review your certificate inventory. For more information, see "[Review your certificate inventory.](#)" on page 53

Quick Start Configuration Overview for Local Certificate Management

The following steps provide a quick overview of the procedures required to configure and enable the local certificate management features in Trust Protection Platform.

1. Configure the Trust Protection Platform Agent's certificate discovery settings.

The Agent certificate discovery settings determine the time at which the local Agent scans the local system for certificates. Additionally, you can designate the directories or keystores that you want to include or exclude from the discovery scan, provide the passwords necessary to access those keystores, and define the types of files you want to discover. In the case of the Windows CAPI keystore, you can even determine which part of the keystore you want the client to scan. The Agent certificate discovery configuration also defines the Discovery object where the Agent's certificate discovery results are stored on the Trust Protection Platform server.

You can implement the Agent's certificate discovery settings on a global level using the Agent Modules in the Platform tree, or you can individually configure the Trust Protection Platform Agents at the local machine using a command line interface.

2. Configure the Base Agent object in the Platforms tree.

The Base Agent object defines the general Trust Protection Platform Agent settings such as the IPv4 or IPv6 address and port where Agents connect and the schedule for Trust Protection Platform Agents to connect to the Trust Protection Platform Server. For information on configuring the Base Agent, see in the *Venafi Trust Protection Platform Administration Guide*

3. To define global Agent certificate discovery settings, configure the Server Agent's Certificate Module on the Trust Protection Platform server. The Certificate Module determines the time at which the Trust Protection Platform Agent runs its scan as well as the time that it reports the discovery results. Additionally, you can designate the directories or keystores that you want to include or exclude from the discovery scan and map file extensions to specific keystore types. When the Server Agents check in with the Trust Protection Platform server, they download the configuration parameters defined in the Agent Modules.
4. After you install the Trust Protection Platform Agent on your local machines, you can use the Trust Protection Platform Agent command line interface to implement settings unique to a specific machine. For example, you can provide the credentials required to access the keystores on that workstation. For more information, see [Server Agent command line reference](#).
5. Install the Trust Protection Platform Agent on the machines where you want to discover certificates in the local file system or keystores.

After installation, the Agent automatically performs its discovery scans as per the schedule and parameters defined in the Agent configuration. Certificate discovery results are uploaded to the Trust Protection Platform server and stored in the designated Discovery object.

For information on installing the Trust Protection Platform Server Agent, see [—Introduction](#) in the *Installing and Configuring the Venafi Agent Guide*.

6. Bring the discovered certificates under management.

You can view the cumulative results of all the workstation certificate discovery scans in the designated Discovery object in the Discovery tree. The discovery results provide an inventory of certificates in your network environment.

NOTE By default, all certificate discovery results are stored in the Certificate Module Discovery object in the Discovery tree.

In the discovery results page, you can determine which certificates you want to bring under management for monitoring. Currently, Trust Protection Platform discovers and monitors certificates for expiration notifications. Monitoring certificates provides an easy, centralized way to track your certificate inventory.

7. Configure your certificate expiration Notification Rules.

8. Notification Rule objects allow you to receive notifications when a certificate nears expiration. The Notification Rule stores the criteria the Venafi Log server uses to select expiration events and designates which Channel objects the Log server uses to provide event responses.

For information on defining Notification Rules, see "[Creating notification rules](#)" on page 432 in the *Venafi Trust Protection Platform Administration Guide*.

9. Configure and generate the Expiration report.

10. The Expiration Report shows all certificates that have expired or will be expiring within the timeframes designated in the report configuration. The report configuration also determines report format, delivery

options, and how often the report is generated. You can also define the report recipients. Each time the report generates, Trust Protection Platform can automatically send the report to designated recipients or the administrative contacts for each encryption asset listed in the report. For more information, see [Certificate Expiration Report](#).

11. Review your certificate inventory.

Trust Protection Platform provides several ways to track your certificate inventory (SSL and client).

The Dashboard view in the Windows and Policy Trees provides a quick view of the total number of managed certificates.

The Policy object's View tab provides a listing of the policy's subordinate certificates and their associated common name, issuer, and expiration date. This list can be sorted and filtered for analysis—for example, to display all certificates issued by a particular CA.

For more information, see ["Opening the certificate inventory" on page 37](#).

2

Discovering certificates and keys

The first step in managing your organization's encryption environment is to determine which encryption assets are deployed where. There are several methods for discovering and provisioning certificates and keys, and for managing them once they are found.

You can use TLS Protect to create several job types you can use to automate tasks, such as certificate and key discovery, import, placement and provisioning. For example, you can create network discovery jobs to get a complete list of your network certificates and SSH keys.

- **Bulk Provisioning:** installs many certificates and keys on your devices at the same time while minimizing device interactions. Requires that your administrator loads a PowerShell script for your type of device. See the Installing (provisioning) certificates and keys in bulk in the *Certificate Management Guide*.
- **Certificate and Device Placement:** use to reconcile duplicates and organize certificates and devices in folders based on rules you specify. See "[Certificate and Device Placement jobs](#)" on [page 96](#) in the *Certificate Management Guide*.
- **Certificate Import:** bring certificates under management that are issued by a specific CA. See Configuring a certificate import from a Microsoft CA in the *Administration Guide* and [POST Discovery/Import](#) in the *Developer's Guide*.

- **Kubernetes Discovery:** use to discover and monitor TLS certificates used by Kubernetes (and most major distributions) clusters managed by Venafi TLS Protect for Kubernetes. See ["Using Kubernetes discovery" on page 83](#) in the *Certificate Management Guide*.
- **Network Discovery:** discover where all of your SSL certificates and SSH keys are deployed in your network and apply placement rules you create to ensure that discovered certificates and keys are organized the way that you want them. See ["Creating a network discovery job" on page 58](#) in the *Certificate Management Guide*.
- **Onboard Discovery:** automates the process of importing certificates into Trust Protection Platform from network devices where you can then monitor, validate, and provision them. See ["Using Onboard Discovery" on page 70](#) in the *Certificate Management Guide*.
- **Server Agent-based discovery:** deploy Server Agents to servers and clients and then configure certificate and SSH key discovery work. See [Server Agent—Introduction](#) in the *Certificate Authority and Hosting Platform Integration Guide*. To learn more about SSH key discovery, see [Running an SSH discovery: finding devices and SSH keys](#) in the *Certificate Management Guide*.
- **Scanafi:** uses the WebSDK with the Scanafi utility to discover network certificates and then adds the certificates to a policy folder automatically. See [Automatically calling Discovery/Import from Scanafi](#) in the *Developer's Guide*.

DID YOU KNOW? Items not already under management can be brought under management, or you can leave them in an *unassigned* policy. To learn more, see ["Unassigned certificates" on page 27](#) in the *Venafi Trust Protection Platform Certificate Management Guide*.

You can also import certificates from a specific certificate authority (CA). To learn more, see ["Importing certificates from a certificate authority" on page 117](#).

This chapter contains the following topics:

Using network discovery	57
Using Onboard Discovery	70
Using Instant Discovery	83
Using Kubernetes discovery	83
Organizing discovered certificates and keys	87
Certificate and Device Placement jobs	96

Managing discovery jobs	103
About placement of duplicate certificates	111
Moving certificates and keys in bulk after Discovery	112
Enabling a discovery placement engine	115
Specifying discovery exclusion objects	115

Using network discovery

Venafi Trust Protection Platform™'s Network Discovery feature provides an easy and convenient way to inventory your network's SSL certificates and SSH server keys.

During a network discovery, the Discovery server scans designated IPv4 address ranges and ports to identify SSL certificates or SSH public keys. You can also perform an instant discovery on an individual IPv4 or IPv6 address and port. During the scan process, Trust Protection Platform sends SSL and SSH requests to the target ports at the designated IP addresses. If the server responds, Trust Protection Platform retrieves the server's certificate or SSH public key.

NOTE *Instant Discovery* retrieves only the certificate information; however, you are given the option of bringing the discovered certificate under management.

Network Discovery identifies where SSL certificates and SSH servers are deployed and provides valuable information. In the case of network SSL certificates, the discovery scan identifies the certificate common name (CN), the IP address of the server where the certificate is located, the certificate expiration date, and the CA. In the case of SSH server keys, the network discovery identifies where SSH servers are deployed and whether those servers are configured in compliance with corporate folders, including key lengths, protocol versions, supported authentication methods and other information.

The discovery results update each time the discovery runs, giving you a centralized, always-current inventory of certificates, SSH systems, configuration information, keys and trust relationships.

As discovery runs, it can place the discovered certificates and public SSH server keys under management in Trust Protection Platform. This is the fastest and easiest way to bring encryption assets under management. This placement happens for items as they are discovered, thus during a discovery it is not uncommon to see items appear in management before the discovery job is complete.

Creating a network discovery job

You can create Network Discovery jobs that scan specific IP addresses, CIDRs, hostnames, and ports to locate certificates. Network discovery jobs can be run on demand or according to a customized schedule (see "Scheduling a job" on page 105 in the *Trust Protection Platform Certificate Management Guide*).

When the Venafi SSH Protect product is installed in your environment, you should be aware of the following items:

- When the placement rules portion of a discovery is run, device objects are created and placed into the policy tree in the location specified in the first matching rule.
- The device object has `DN=hostname` of the discovery result.
If there is no hostname, the device's IP address is used as the hostname.
- The hostname or address fields are filled with the full hostname or IP address if there is no other data to enter in these fields.
- If the DN for a discovered device object already exists in the same folder, a duplicate object is **NOT** created; however, if the DN for a discovered object already exists in a different folder, the second device object **IS** created (unless already created by the same job previously).

Both device objects will be present in the tree.

To create a new Network Discovery job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.

(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See "Filtering the Jobs list by job type" on page 104.

2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Network Discovery**, and then click **Start**.
4. In the **Create New Job** window, enter details about the job.
 - **Targets:** Each line can contain a single IP address, a hyphenated range of IP addresses, a CIDR address range, or an individual host name. You can also enter a target in an IP address:Port format, for example, `192.168.1.1:443`.
 - **Placement Rules:** To create a placement rule, click **+ Create New Rule**.

See "Creating placement rules" on page 87 in the *Trust Protection Platform Certificate Management Guide*.

- **Exclusions:** Addresses, ports, CIDRs, and host names that should not be scanned.

See "Specifying discovery exclusion objects" on page 115 in the *Trust Protection Platform Certificate Management Guide*.

Create New Job

Name *

Description

Contacts

Targets

IP, CIDR, and Hostnames (one per line) *

Ports *

80,443-449,465,563,636,695,981-995,1311,1920,2083,2087,2096,211,2484,2949,3268,3269,3414,4712,4843,5223,5358,6619,6679,6697,7002,8080,8222,8243,8333,8443,8878,8881,8882,9043,9090,9091,9443,18072,18080-18085,18090-18094,28080

Exclusions

Placement Rules

Execute rules in this order

Select rule to add

+ Create New Rule

If no rules apply, put results into this policy *

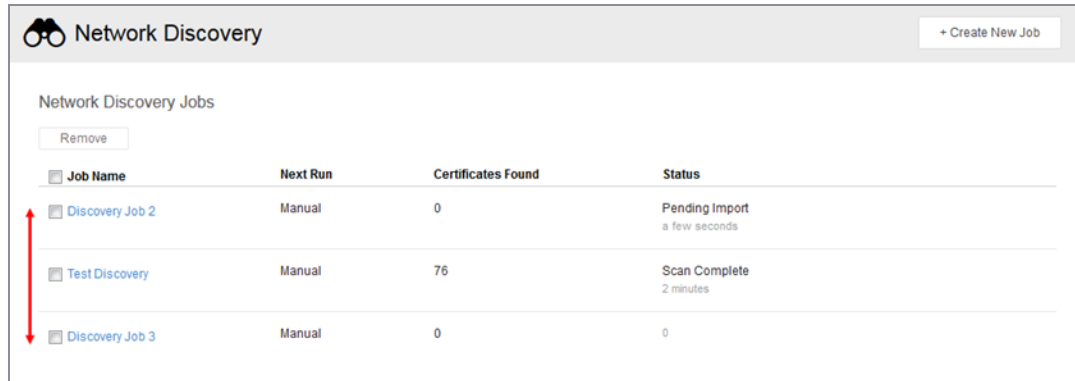
If no rules apply, put results into this policy

Cancel Create & Run Create Job

5. Do one of the following:

- When you're done, click **Create Job**.
- (Optional) If you want to run the job immediately, click **Create & Run**.

Your job list will look something like this:



The screenshot shows a web interface titled "Network Discovery" with a "+ Create New Job" button. Below the title is a section "Network Discovery Jobs" with a "Remove" button. A table lists three jobs. A red double-headed arrow is positioned to the left of the first two jobs, indicating they can be reordered.

☐ Job Name	Next Run	Certificates Found	Status
☐ Discovery Job 2	Manual	0	Pending Import a few seconds
☐ Test Discovery	Manual	76	Scan Complete 2 minutes
☐ Discovery Job 3	Manual	0	0

NOTE When you pause and resume a discovery job, the statistics can show that more things were scanned than you expect. This is normal behavior, a result of the way scan groups are created and processed.

TIP As with placement rules, you can reorder the priority of each job by dragging and dropping it in the list.

Specify a default location if no rules apply

When you create a new job, you *must* specify where items are to be placed when no placement rules apply.

Create New Job

80,443-449,465,563,636,695,981-995,1311,1920,2083,2087,2096,211,2484,2949,3268,3269,3414,4712,4843,5223,5358,6619,6679,6697,7002,8080,8222,8243,8333,8443,8878,8881,8882,9043,9090,9091,9443,18072,18080-18085,18090-18094,28080

Exclusions

Placement Rules

Execute rules in this order

Rule 1

Select rule to add

+ Create New Rule

If no rules apply, put results into this policy *

If no rules apply, put results into this policy

--Select--
Policy
Policy \ EMEA
Policy \ EMEA \ HR
Policy \ EMEA \ HR \ Hurman Resources Europe
Policy \ EMEA \ Mktg

Cancel

Create & Run

Create Job

BEST PRACTICE It's a good idea to make the Management Type of the default policy *unassigned*. You can then move these certificates and keys from the unassigned default policy to their correct managed folders.

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.

Managing the discovery server

To enable Network discovery, you must install the Discovery Module on the servers where you want to deploy the Discovery Manager. Because of its modular architecture, the Discovery module can be independently deployed on one or more servers. Depending on your system requirements, you may run discoveries from a single Trust Protection Platform server or, for larger systems, you may require a dedicated Discovery server. If you scan both private and public IP addresses, you may configure one Discovery Server inside the firewall and another outside the firewall.

The Discovery Module is included in the Venafi TLS Protect and Venafi SSH Protect program installations. During the installation process, you select the Discovery Module in the Installation wizard's Component Selection window. For more information on the installation process, refer to the *Installation Guide*.

After you install the Discovery module, you can set the Discovery Server parameters by configuring the Trust Protection Platform Server object and its associated Discovery module in the Platforms tree.

In the Trust Protection Platform Server object, you define the zones you want the current server to service. The Discovery module runs discoveries only on the zones designated in the Trust Protection Platform Server object.

NOTE A Discovery Zone is a range of Class C or larger IPv4 addresses to which the current server has network access.

This option provides a way to manage which servers process which 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 manage which discoveries run on which server by defining the zones that you want each server to process.

For information on configuring the Trust Protection Platform Server object, see "[Configuring discovery zones](#)" below.

In the Discovery module, you define the Discovery connection settings and processing times. For more information, see [Configuring the Discovery module](#).

NOTE If you are running multiple Discovery Servers with different zones, you must ensure that the addresses defined in the Discovery object fall within one of the Discovery Server's configured zones. Otherwise, any IP addresses not included in the Discovery Server's configured zones are not processed and the Discovery will never be completed. For information on configuring Discovery objects, see .

Configuring discovery zones

The Trust Protection Platform Server object represents a server where one of the Trust Protection Platform products is installed. In the Trust Protection Platform Server object, you can define the Discovery Zones you want the current server to service. If the Discovery module is installed on the current server, it runs discoveries only on the designated discovery zones.

DID YOU KNOW? A Discovery Zone is a range of Class C or higher IPv4 addresses to which the current server has network access.

Defining Discovery Zones on the Trust Protection Platform Server object provides a way to manage which servers process which discoveries.

If you do not define Discovery Zones on the Trust Protection Platform Server object, the Discovery module processes all configured Discovery objects.

To configure the Venafi Trust Protection Platform Server's Discovery Zones

1. From the [TLS Protect 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 object.
You must have the View and Write permissions to the Trust Protection Platform Server object.
4. On the **Venafi Trust Protection Platform > Settings** tab, in the **Discovery Zones** section, click **Add**.
5. In the **Add IP Range** box, type a range of class C or higher IPv4 addresses that you want the current server to service.

The server must have network access to the IP addresses within the designated zone.

6. Configure the Trust Protection Platform Server settings, and then click **Add**.
7. Repeat steps 4 and 5 for every Discovery Zone you want the current server to service.
8. When finished, click **Apply**.

Excluding IP addresses and host names from discovery scans

Exclusion objects define ranges of IPv4 addresses and ports that you do not want the Discovery engine to scan. You can also exclude certificates and SSH server keys already being managed in the Policy tree from discovery, or you can exclude certificates from discovery based on the certificate's Issuer or Subject DN.

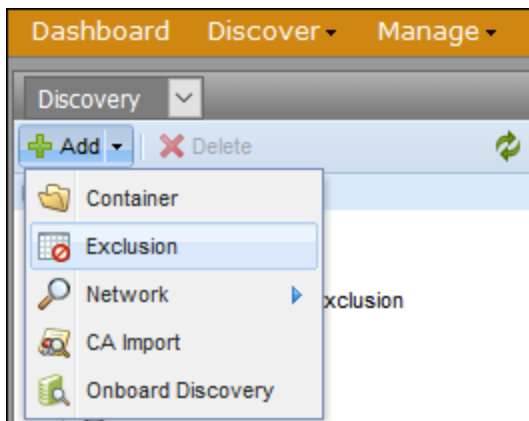
To apply these exclusions to individual discoveries, you must reference the Exclusion objects in the Discovery object configuration. For information on configuring Discovery objects to reference an Exclusion object, see ["Specifying discovery exclusion objects"](#) on page 115.

To create an Exclusion

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

IMPORTANT You must have the *View* and *Create* permissions to the root Discovery object to create Exclusion objects.

2. In the **Discovery** tree, select the root Discovery object or the Discovery folder where you want to create the Exclusion object.
3. Click **Add > Exclusion**.



4. Refer to the following table to configure the remaining settings:

Field	Description
General	
Rule Name	Enter a name for the exclusion.
Description	Custom description for the exclusion
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.

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 (*). Select a User or Group Identity, and then click Select. Press Shift+click to select multiple, contiguous objects. Press Ctrl+click to select multiple, discontinuous objects.
Exclude	Allows you to define the IPv4 addresses and ports you want to exclude from discovery. You can exclude IPv4 addresses with their associated ports, port ranges, or both. If you enter duplicate IPv4 address and port settings in the Exclusion object, the Summary tab duplicates the exclusions in the scan results. For example, if you added the same IPv4 address and port to the Exclusion object four times, the Summary tab would report four ports excluded.
Addresses, Hostnames, definitions	Range of IPv4 addresses that you want to exclude from Discovery. For example, if you want to exclude IP addresses 198.162.0.1 through 198.162.0.100 inclusive, type and/or CIDR 192.168.0.1 in the first text box and 192.168.0.100 in the second text box. If you want to exclude only one device, type the IPv4 address in the first box.
Port Range (s)	Ranges of ports that you want to exclude from discovery on all scanned IPv4 addresses. These addresses and ports will not be scanned by any associated discovery.
Ignore	

Field	Description
Managed DN(s)	Allows you to ignore certificates that are already under management in the designated DNs. When you choose to ignore managed keys found within a designated DN in the Policy tree, those objects are filtered out of the Discovery results. That is, the Discovery engine continues to find them; you just don't see them in the Discovery results. When you specify a DN to ignore, the Discovery Server ignores all certificates from that point down in the Policy tree.
Issuer DN Regular Expression (s)	Excludes a certificate from discovery based on a regular expression applied to the issuer DN (CA). The regular expression is used only to exclude certificates from the discovery. It cannot be used to select certificates. For example, if your system has HP LaserJet printers, you can use the following regular expression to exclude HP LaserJet certificates from discovery: O=Hewlett-Packard\sCo.,\sCN=HP\sJetdirect If you want to do a simple "contains" statement, you can enter: Jetdirect
Subject DN Regular Expression (s)	Excludes a certificate from discovery based on a regular expression applied to the subject DN. For example, the following regular expression excludes from discovery all certificates issued to NonCorp.com: (cn=.*?noncorp.com.* dc=noncorp.*) If you want to do a simple "contains" statement, you can enter: noncorp.com The regular expression is used only to exclude certificates from the discovery. It cannot be used to select certificates.

- When you're finished, click **Save**.

Next step: ["Specifying discovery exclusion objects" on page 115](#)

About network discovery objects

Network Discovery objects in the Discovery tree provide the information that Trust Protection Platform requires to run network discoveries.

The following sections outline how to create and configure discovery objects in the Discovery tree.

Exclusion object settings

Exclusion objects are referenced in the Discovery object configuration to apply the exclusions to individual discoveries.

Field	Description
General	
Rule Name	Enter a name for the exclusion.
Description	Custom description for the exclusion
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 objects. Press Ctrl+click to select multiple, discontinuous objects.
Exclude	Allows you to define the IPv4 addresses and ports you want to exclude from discovery. You can exclude IPv4 addresses with their associated ports, port ranges, or both.

Field	Description
	If you enter duplicate IPv4 address and port settings in the Exclusion object, the Summary tab duplicates the exclusions in the scan results. For example, if you added the same IPv4 address and port to the Exclusion object four times, the Summary tab would report four ports excluded.
Address, Hostname, and/or CIDR definitions	Range of IPv4 addresses that you want to exclude from Discovery. For example, if you want to exclude IP addresses 198.162.0.1 through 198.162.0.100 inclusive, type 192.168.0.1 in the first text box and 192.168.0.100 in the second text box. If you want to exclude only one device, type the IPv4 address in the first box.
Port Range (s)	Ranges of ports that you want to exclude from discovery on all scanned IPv4 addresses. These addresses and ports will not be scanned by any associated discovery.
Ignore	

Field	Description
Managed DN (s)	Allows you to ignore certificates that are already under management in the designated DNs. When you choose to ignore managed keys found within a designated DN in the Policy tree, those objects are filtered out of the Discovery results. That is, the Discovery engine continues to find them; you just don't see them in the Discovery results. When you specify a DN to ignore, the Discovery Server ignores all certificates from that point down in the Policy tree.
Issuer DN Regular Expression (s)	Excludes a certificate from discovery based on a regular expression applied to the issuer DN (CA). The regular expression is used only to exclude certificates from the discovery. It cannot be used to select certificates. For example, if your system has HP LaserJet printers, you can use the following regular expression to exclude HP LaserJet certificates from discovery: O=Hewlett-Packard\sCo.,\sCN=HP\sJetdirect If you want to do a simple "contains" statement, you can enter: Jetdirect
Subject DN Regular Expression (s)	Excludes a certificate from discovery based on a regular expression applied to the subject DN. For example, the following regular expression excludes from discovery all certificates issued to NonCorp.com: (cn=.*?noncorp.com.* dc=noncorp.*) If you want to do a simple "contains" statement, you can enter: noncorp.com The regular expression is used only to exclude certificates from the discovery. It cannot be used to select certificates.

Using Onboard Discovery

The Onboard Discovery feature automates the process of importing certificates into Trust Protection Platform from network devices where you can then monitor, validate, and provision them.

When you configure and run a new onboard discovery job, applications are added to one or more specific devices automatically. You then have control over the placement of discovered certificates without having to manually update jobs or reorganize certificates after they've been discovered.

By providing Trust Protection Platform with the hostnames or addresses and credentials of your network devices, all appliance certificates in current use are brought into Trust Protection Platform along with required application configuration settings. This immediately puts the discovered certificates under the protection of TrustForce.

DID YOU KNOW? Agentless Onboard Discovery is currently available for the following devices (Installation Types):

- **Adaptable Onboard Discovery**
You can select this installation type for devices that are not directly supported by Onboard Discovery. You'll need to create your own PowerShell script.
- Amazon Web Services
- Azure Key Vault
- Citrix NetScaler
- F5 Big-IP Local Traffic Manager (F5 LTM Advanced)
- IBM DataPower
- Microsoft IIS (CAPI)

Onboard Discovery prerequisites

Before running an onboard discovery, review the following:

- Make sure that the devices to be analyzed are compatible with the software platform versions and that any platform-specific prerequisites are met.
- Make certain that all devices are configured with a device credential, which is used by Trust Protection Platform to authenticate with each device.

IMPORTANT For a discovery job to complete successfully, the correct HostName/IP and device credentials must be set on the devices to be scanned. Not doing so results in a device scan failure and a corresponding error is logged in the Onboard Discovery object log.

General permissions (Required)

Venafi Trust Protection Platform requires a sufficient level of permissions to export certificates and read certificate-related details from the device configuration. The specific permissions requirements and mechanism used to provide them varies by the platform to be scanned.

Connectivity requirements are the same as they are for provisioning using the HTTPS connection method (for F5, NetScaler, and DataPower).

Specific requirements

Click to expand the installation type you plan to use with Onboard Discovery and carefully review the requirements before creating your new job.

Adaptable

Similar to the Adaptable Application used for provisioning, the Adaptable application type requires that you first create a PowerShell script that implements the Discover-Certificates function and save it in the `<Venafi_Home>\Scripts\AdaptableApp` directory of the Trust Protection Platform server.

After creating and saving your script to the correct directory, you must assign it by policy to the folder containing the device objects to be scanned by selecting it from the policy's PowerShell Script list (*policy* > **Applications** > **Adaptable** sub-tab). For more information, see [Assigning the PowerShell script to a policy](#).

NOTE Adaptable imports certificates but does not import keys.

For more information about the Discover-Certificates function, see [Discover-Certificates function](#). For more information about the Adaptable Framework and PowerShell scripting, see [PowerShell script reference for Adaptable Application](#).

Amazon Web Services

If you're using Amazon Web Services (AWS) as your installation type, do the following before you create your onboard discovery job:

- Review AWS permission requirements.

See [AWS permission requirements](#).

- Create an Amazon credential.

When configuring your onboard discovery job, you'll need to select your Amazon credential.

See [Creating and editing an Amazon Credential in the Trust Protection Platform Administration Guide](#).

- Create a policy folder that where discovered AWS certificates and installations can be placed.

See [Creating policies in the Trust Protection Platform Administration Guide](#).

Azure Key Vault

If you're using Microsoft Azure Key Vault as your installation type, do the following before you create your onboard discovery job:

- Review Azure permission requirements.

See [Azure permission requirements](#).

- Create a certificate credential.

When configuring your onboard discovery job, you'll need to select a certificate credential.

See [Creating credential objects in the Trust Protection Platform Administration Guide](#).

- Create a policy folder where discovered Azure Key Vault certificates can be placed.

See [Creating policies in the Trust Protection Platform Administration Guide](#).

CAPI (IIS Bindings)

Use this application type to specifically discover Internet Information Service (IIS) bindings *only* (available websites and corresponding certificates). All other certificates in CAPI are excluded.

Each binding that is discovered is represented in Trust Protection Platform by a new CAPI application object and an associated certificate.

For prerequisite information, refer to the Venafi CAPI driver topic, [CAPI driver prerequisite configuration](#).

Citrix NetScaler

Onboard Discovery interfaces with Citrix NetScaler devices using their Nitro API, which is supported by Citrix NetScaler 10.5 (or higher).

For prerequisite information, refer to the Venafi NetScaler driver topic, [NetScaler prerequisite configuration](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

F5 Big-IP Local Traffic Manager (F5 LTM Advanced)

Onboard discovery interfaces with F5 LTM Advanced devices using their iControl REST API, which is fully supported by versions 11.5 (or higher) of the F5 Networks product.

F5 LTM Advanced Permissions: At minimum, the user account used by Trust Protection Platform to access your F5 device must have the Administrator role, which can be assigned to a local user or a Remote Role Group for a non-local user. This is because the Administrator role is the least privilege required for interfacing with the iControl REST API.

IBM WebSphere DataPower

Onboard Discovery interfaces with DataPower devices, versions 7.2 (or higher), because those are the versions that support a REST API.

For prerequisite information, refer to the Venafi DataPower driver topic, [IBM WebSphere DataPower prerequisite configuration](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Creating a new Onboard Discovery job

When configuring onboard discovery jobs, you can select any number of device objects from the Policy tree. Alternatively, you can choose to recursively search a folder for device objects to add before any job begins the actual process of scanning.

TIP Before you create your onboard discovery job, make sure that you've carefully reviewed ["Onboard Discovery prerequisites"](#) on page 70.

To create a new Onboard Discovery job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.

(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See ["Filtering the Jobs list by job type"](#) on page 104.

2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Onboard Discovery**, and then click **Start**.
4. Under **Job Details**, in the **Name** field of the **New Onboard Discovery Job** page, type a name for your new onboard discovery job.
5. (Optional) In the **Description** field, type a description that describes the purpose for 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.

6. (Optional) In the **Contacts** field, begin typing the name a user name to specify one or more contacts for your new job.

To add multiple contact names, press **Enter** after finding each name.

7. From the **Installation Type** list, select one of the available types.

Continue by viewing the configuration details for the installation type you chose:

- **Adaptable**

(Optional) If you want to enhance troubleshooting capabilities of your Adaptable Onboard DiscoveryAdaptable Flow, select the **Enable Debug Logging** check box.

For information about how enabling this option works with the PowerShell script, see [About debug logging](#) in the Adaptable ApplicationAdaptable Flow PowerShell script reference.

For the **Adaptable** installation type, if you want to enhance troubleshooting capabilities of your Adaptable Log Channel implementation, select the **Enable Debug Logging** check box.

You should have already created your PowerShell script and placed it in the correct folder. If you haven't done that yet, stop here and review "[Specific requirements](#)" on page 71 and "[Adaptable Onboard Discovery sample script](#)" on page 80.

- **Amazon Web Services**

If you selected **Amazon Web Services**, then from the **Amazon Credentials** field, select an Amazon Credential.

If you don't see your credential in the list, type the first few characters of the credential's name.

For information about creating your credential, see [Creating and editing an Amazon Credential](#).

(Optional) Select **Do not discover binding targets (ELB, ALB, CloudFront)** if you want Trust Protection Platform to skip the discovery of binding targets such as Elastic Load Balancers, Application Load Balancers, and Cloud Front.

NOTE Only load balancers with 'Load Balancer Protocol' set to HTTPS will be discovered.

◦ **Azure Key Vault**

If you selected **Azure Key Vault**, do the following:

- Click the **Azure Certificate Credential** field to select an Azure credential.

If you don't see your credential in the list, type the first few characters of the credential's name.

TIP If you're not sure about your Azure Key Vault credential, you might have [missed that step](#).

- Copy and paste your application ID into the **Azure Application ID** field.

◦ **CAPI (IIS Bindings)**

If you selected **CAPI (IIS Bindings)** as the application type, then using the fields that appear when you selected this type, do the following:

- In the **WinRM Port** field, type the WinRM port number.

The default setting is 5986.

- (Optional) Select **Extract private keys with certificates when possible** if you want Trust Protection Platform to attempt to extract private keys from the device along with certificates and store them with the same object.

When this option is enabled, a warning event is logged whenever a private key cannot be extracted.

NOTE Private keys can only be extracted if they are not stored inside a hardware security module (HSM) and are exportable.

TIP If you intend keys to be generated remotely on the device—and therefore not accessible by Trust Protection Platform users—then you don't likely need this option.

DID YOU KNOW? During an onboard discovery, Trust Protection Platform only imports the private keys for certificates that do not already exist in the Policy folder. In cases where you need to extract the private key for a certificate that already exists in the Policy folder, then delete the existing certificate from that folder and re-run the onboard discovery job.

◦ Citrix NetScaler

If you selected **Citrix NetScaler** as the profile type, then using the fields that appear when you selected this type, do the following:

- From the **Certificates to Import** list, select the certificate types to import (**Only Virtual Servers**, **Only Gateway Virtual Servers**, **Only Services and Groups**, or **All**).

DID YOU KNOW? Trust Protection Platform 22.2 added support for discovery of virtual servers, services, and service groups in admin partitions.

- In the **Keystore and Private Key Credentials** field, select the password credentials required for any PFX files that might be encountered.

This option is also used to decrypt password-encrypted private keys when they're encountered, *if* you also enable **Extract private keys with certificates when possible** option.

- (Optional) Select **Extract private keys with certificates when possible** if you want Trust Protection Platform to attempt to extract private keys from the device along with certificates and store them with the same object.

When this option is enabled, a warning event is logged whenever a private key cannot be extracted.

NOTE Private keys can only be extracted if they are not password encrypted, can be decrypted using one of the passwords assigned to **Keystore and Private Key Credentials** of the job, or not stored inside a hardware security module (HSM).

TIP If you intend keys to be generated remotely on the device—and therefore not accessible by Trust Protection Platform users—then you don't likely need this option.

DID YOU KNOW? During an onboard discovery, Trust Protection Platform only imports the private keys for certificates that do not already exist in the Policy folder. In cases where you need to extract the private key for a certificate that already exists in the Policy folder, then delete the existing certificate from that folder and re-run the onboard discovery job.

◦ F5 LTM Advanced

If you selected **F5 LTM Advanced**, then using the fields that appear when you selected this type, do the following:

- From the **Certificates to Import** list, select the certificate types to import (server, client, or both).

- In the **Port** field, type the port number.

The default setting is 443.

- (Optional) Select **Extract private keys with certificates when possible** if you want Trust Protection Platform to attempt to extract private keys from the device along with certificates and store them with the same object.

When this option is enabled, a warning event is logged whenever a private key cannot be extracted.

NOTE Private keys can only be extracted if they are not password encrypted nor stored inside a hardware security module (HSM).

TIP If you intend keys to be generated remotely on the device—and therefore not accessible by Trust Protection Platform users—then you don't likely need this option.

DID YOU KNOW? During an onboard discovery, Trust Protection Platform only imports the private keys for certificates that do not already exist in the Policy folder. In cases where you need to extract the private key for a certificate that already exists in the Policy folder, then delete the existing certificate from that folder and re-run the onboard discovery job.

- (Optional) Select **Disable certificate installations not in use** so when the next F5 onboard discovery job runs, it will disable and make obsolete the previously-discovered certificate installation, which no longer corresponds with the newly-discovered F5 configuration. The certificate installations are renamed and still exist in Trust Protection Platform.

Use case: An example for using this option is when you have a discovery on certificate installations, and another team responsible for F5 management manually switches an SSL profile associated with a virtual server to a different virtual server. On the next discovery, the F5 Discovery Job discovers the new SSL profile and certificate. If this option is left unchecked, Trust Protection Platform maintains the previous certificate installation, which no longer exists in the F5 environment. If the prior certificate is then auto-renewed, it will be provisioned to the F5 environment, updated, and configured on the virtual server. This action will effectively reverse the change made by the F5 team.

- **IBM WebSphere DataPower**

If you selected **IBM WebSphere DataPower** as the profile type, then using the fields that appear when you selected this type, do the following:

- From the **Configurations to Import** list, select the configuration types to import (**TLS Client Profile**, **TLS Proxy Profile**, **TLS Server Profile**, or **Crypto Identification Credentials**).
- In the **REST Port** field, type the port that Trust Protection Platform should use to communicate with your appliance.

The default HTTPS/REST port assignment is port 5554, which applies to the REST API.

8. Click **Next**.

9. Depending on which installation type you selected, then on the **Targets** page, do one of the following:

- a. (Conditional) If you selected any installation type other than Amazon Web Services or Azure Key Vault, then in the **Devices to Scan** field, select the devices that you want scanned, and then continue to the next step.
- b. (Conditional) If you selected **Amazon Web Services** as the installation type, then in the **Account IDs to scan** field, type (or copy in) one or more AWS account IDs, press **Enter** after each ID, then specify the AWS regions where you want to allow the discovery, and then [skip down to the Placement Rules step](#).

- c. (Conditional) If you selected **Azure Key Vault** as the installation type, type your tenant ID in the **Azure Tenant ID** field, and then [skip down to the Placement Rules step](#).
10. (Conditional) If you haven't yet created device objects, click **Create New Devices** and then do one of the following:
 - a. If you already have the required credential, click **Create New Device Only** and do the following:
 - i. In the **Device Addresses** field, type one or more new device addresses.

TIP When working with many devices, you can copy and paste all of the addresses into this field at once, provided that you include commas between each address.
 - ii. In the **Device Folder** field, begin typing the name of the folder where you want the devices placed and select a folder.
 - iii. In the **Credential** field, begin typing the name of the credential to use and then select it.
 - iv. When you're finished, click **Save**.
 - b. If you haven't yet created devices or credentials, click **Create New Device and New Credentials**, and then do the following:
 - i. In the **Device Addresses** field, type one or more new device addresses.
 - ii. In the **Device Folder** field, begin typing the name of the folder where you want the devices placed and select the folder.
 - iii. In the **Credential Name** field, type a unique name for your new credential.
 - iv. In the **Credential Folder** field, begin typing the name of the folder where you want the devices placed and select the folder.
 - v. In the **Password** fields, type a password twice to confirm, and then click **Save**.
11. (Optional)(Conditional) If you have a specific folder where all of your devices are located, then select a folder from the **Scan all devices located in this folder (and its subfolders)** field.

All sub-folders of the folder you select are also scanned.
12. Click **Next**.
13. Under **Placement Rules**, do one of the following:
 - (Conditional) If you selected Amazon Web Services or Azure Key Vault, select the folder where you want discovered certificates and applications to be placed, and then click **Next**.

IMPORTANT If a certificate is assigned to a web application but there is no Azure Key Vault available, the Azure Key Vault name value of the associated application object is left empty. In this case, in order to provision successfully after onboard discovery job runs, you'll need to set that value manually.

- (Conditional) If you're configuring any other installation types besides Amazon Web Services or Azure Key Vault select one of the following methods for placing newly discovered certificates:
 - Select **With this device** if you want all newly discovered certificates placed in the same folder where the device is located.
 - Select **In this folder** if you want to select an existing folder where Trust Protection Platform should place all newly discovered certificates.
 - If you're configuring for Amazon Web Services, placement targets must be unique for each AWS Onboard Discovery job that runs concurrently in the Amazon Web Services section.
14. On the **Occurrence** page, specify when you want the new job to run, and then either click **Create & Run** to save your changes and run the job immediately, or click **Create Job** if you plan to run the job at a later time (or have scheduled it to run later).
 15. Click **Save**.

Adaptable Onboard Discovery sample script

You can configure an Adaptable Onboard Discovery job using a PowerShell script as the installation type, rather than using one of the other third-party applications available with Onboard Discovery. You just need to create your script, save it to the correct directory on your Trust Protection Platform server, and set up and configure the associated device object and policy. For more details, see ["Onboard Discovery prerequisites" on page 70](#).

This topic contains a sample script designed to create an Adaptable and Apache application for two different certificates.

In the following example, the Adaptable application will be SSL/TLS-validated at service.venafi.example:44300 and the Apache application will have SSL/TLS validation disabled.

TIP When creating an Adaptable Onboard Discovery job, you are not prompted to specify the location of your script. You must specify your script in the policy object where the device to be scanned is kept.

This is because the primary goal of Onboard Discovery is to enable turnkey provisioning after certificates are discovered and to do that for Adaptable requires that you specify a script by policy to that folder.

After each object is created, the specified attribute values are assigned. If an invalid class is specified, then a Basic application is created and an error event is logged for the onboard discovery job. If a name collision occurs with a Basic application, it is then converted to the specified application class (if valid). If an attribute is not valid for the class, or the value is not a distinguished name (DN) for a DN attribute, then no value is assigned to the application and an error event is logged for the onboard discovery job.

Adaptable Onboard Discovery Sample Script

```

1  function Discover-Certificates
2  {
3      Param(
4          [Parameter(Mandatory=$true,HelpMessage="General Parameters")]
5          [System.Collections.Hashtable]$General
6      )
7
8      ### code for retrieving certificates and instance data from remote device
      goes here ###
9
10     return @{
11         Result = "Success";
12         Applications = @(
13             @{
14                 Name = "virtual_server_1 (ssl_profile_1)";
15                 PEM = "-----BEGIN CERTIFICATE-----MIIEpTCCA42gAwIBAgIJA0w7-----END
CERTIFICATE-----";
16                 ValidationAddress = "service.venafi.example";
17                 ValidationPort = "44300";
18                 Attributes = @{
19                     "Text Field 1" = "virtual_server_1";
20                     "Text Field 2" = "ssl_profile_1";
21                     "Option 1" = "1"
22                 }

```

```

23     },
24     @{
25         Name = "file_path_name (host_address:port:server_name)";
26         ApplicationClass = "Apache";
27         PEM = "-----BEGIN CERTIFICATE-----MIIEpTCCA42gAwIBAgIJALjX-----END
CERTIFICATE-----";
28         Attributes = @{
29             "Certificate File" = "/opt/apache/website.crt";
30             "Private Key File" = "/opt/apache/website.key";
31             "Certificate Chain File" = "/opt/apache/website.chain";
32             "Private Key Password Credential" =
"\VED\Policy\Credentials\Private Key Password"
33         }
34     }
35 )
36 }
37 }

```

For details about the related function, see [Discover-Certificates](#) function.

About debug logging

When a user has requested debug logging by checking **Enable Debug Logging** for Adaptable Onboard Discovery, 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 Onboard Discovery, see .

Using Instant Discovery

In the classic policy tree, you can perform an instant discovery on an individual IPv4 or IPv6 address and port to discover SSL certificates. During the scan process, Trust Protection Platform sends SSL and SSH requests to the target ports at the designated IP addresses. If the server responds, Trust Protection Platform retrieves the server's certificate or SSH public key.

You can also run discovery jobs manually. For more information, see ["Manually running, canceling, or pausing a discovery job" on page 110](#).

To perform a quick discovery in Classic Policy Tree

1. From the menu bar, click **Classic Policy Tree**.
2. To the right of the tree drop-down, click the **Instant Discovery** button.
3. In the **Host Name / IP Address**, type either a fully qualified domain name or IP address of the target system.
4. In the **Port** field, type the port on which an application that's using SSL is currently running.
The default port is 443.
5. Click **Discover**.

Using Kubernetes discovery

Venafi Trust Protection Platform™'s Kubernetes discovery feature provides an easy and convenient way to monitor TLS certificates used on clusters managed by Venafi TLS Protect for Kubernetes module of the Venafi Control Plane. Certificates used in traditional devices and Kubernetes clusters will have operational status visibility and enforceable policy control to all Kubernetes clusters.

With the Kubernetes discovery feature, administrators will be able to create a new discovery job which imports certificates from all Kubernetes clusters registered to Venafi Control Plane. Once discovered, certificates are placed in containers (similar to policy folders) in corresponding clusters and namespaces. As an administrator you can apply policies to each container, cluster, or a namespace.

Non-compliant certificates can be found on the certificate inventory page in TLS Protect which provides a way to filter them by specifying a particular cluster, namespace, or container. Certificates which are used on Kubernetes clusters and are issued by Venafi Trust Protection Platform will be associated with the corresponding cluster and namespace objects. This allows administrators to see where they are used and what Kubernetes services are at risk.

Kubernetes Discovery jobs need network access to Venafi Control Plane to discover certificates within Kubernetes environments. To ensure Venafi Trust Protection Platform™ has access to Venafi Control Plane, customers need to add these endpoints to their network allowlist.

Venafi Control Plane Endpoints:

- EU Region: api.venafi.eu
- US Region: api.venafi.cloud

Required Access

- Port: TCP 443
- Protocol: HTTPS

Creating a new Kubernetes Discovery job

When configuring Kubernetes discovery jobs, you will first need to create a Venafi Control Plane service account.

To create a new Kubernetes Discovery job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See "[Filtering the Jobs list by job type](#)" on page 104.
2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, select **Kubernetes Discovery**, and then click **Start**.
4. Under **Job Details**, in the **Name** field of the **New Kubernetes Discovery Job** page, type a name for your new Kubernetes Discovery job.
5. (Optional) In the **Description** field, type a description that describes the purpose for 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.

6. (Optional) In the **Contacts** field, begin typing the name a user name to specify one or more contacts for your new job.

To add multiple contact names, press **Enter** after finding each name.

7. (Conditional) If you do not have an existing Venafi Control Plane service account, follow the instructions for [Creating a Service Account](#).

NOTE ED25519 keys are not supported.

8. Next, configure the job settings.
 - a. Indicate from which Kubernetes cluster you want to discover certificates. If you will only be discovering from selected clusters, use the controls to move the clusters into the **Selected clusters** box.
 - b. Select if you want to ignore certificates from inactive clusters.
Clusters are considered inactive when they do not report data to Venafi Control Plane, but they are still registered.
 - c. Select if you want to include expired certificates.
 - d. Specify the minimum validity of the certificates which you want to discover.
 - e. Using the drop-down box select a folder where the discovered clusters and certificates should be placed.
 - f. In the **Retirement** section, select how the system should handle deleted Kubernetes clusters.

Clusters are considered deleted when removed from Venafi Control Plane. Based on your selection, the following details apply:

- **Delete** - When clusters are deleted from Venafi Control Plane, they will be removed from the Venafi Trust Protection Platform Inventory and their related certificates will be deleted if they are not associated with other applications, Kubernetes clusters, or namespaces. If there are certificates associated with another Kubernetes cluster or application, they are automatically moved into a new Kubernetes policy folder labeled **Associated Certificates**

(**automatically moved**) under the same organization.

- **Move** - When clusters are deleted from Venafi Control Plane, they will be moved to a new location. If their related certificates are associated to another application, Kubernetes cluster, or namespace, they will be moved to **Associated Certificates (automatically moved)**. Otherwise, they will be moved to **Archived**.

g. Next, select how the system should handle deleted certificates.

- **Retire** - When certificates are deleted from the Kubernetes cluster, certificates monitoring is disabled if the certificates are not in use by another application, Kubernetes cluster, or namespace. Certificates that are in use by another cluster or application are automatically moved to a new Kubernetes policy folder labeled **Associated Certificates (automatically moved)** and are not retired.
- **Revoke** - When certificates are deleted from the Kubernetes cluster, and they are issued by Venafi, a revocation is requested if the certificates are not in use by another application, Kubernetes cluster, or namespace. Certificates that are in use by another cluster or application are automatically moved to a new Kubernetes policy folder labeled **Associated Certificates (automatically moved)** and revocation is not requested.
 - Specify certificate revocation for a number of days. In the event that a certificate is deleted from the Kubernetes cluster, it will not be immediately revoked for a specified period of time, but rather will be kept in a monitoring state during that time. This intentional delay is to allow time for any dependent systems or applications to be updated and avoid disruption. After the specified period of time, the certificate would then be revoked if it has not been reissued or renewed.
- **Delete** - When certificates are deleted from the Kubernetes cluster, they are removed from the inventory if the certificates are not in use by another application, Kubernetes cluster, or namespace. Certificates that are in use by another cluster or application are automatically moved to a new Kubernetes policy folder labeled **Associated Certificates (automatically moved)**.
- **Move** - When certificates are deleted from the Kubernetes cluster, they are moved to the specified location if the certificates are not in use by another application, Kubernetes cluster, or namespace. Certificates that are in use by another cluster or application are automatically moved to a new Kubernetes policy folder labeled **Associated Certificates (automatically moved)**.

h. Click **Next**.

9. Finally, select the frequency of when you would like the job to run.
10. Click **Create Job**.

Organizing discovered certificates and keys

You can create rules to determine the placement of certificates and SSH keys that are found during discovery. You do this using *placement rules*.

Creating placement rules

When you set up placement rules, Trust Protection Platform automatically follows those rules, in order, from top to bottom, to place keys, certificates, and their corresponding devices into folders.

IMPORTANT If network discovery finds a new version of a certificate that is already in the database, it combines the certificates, putting the older certificate in the certificate history of the newer certificate. For more information, see ["About placement of duplicate certificates" on page 111](#).

To create one or more placement rules

1. From the **TLS Protect menu bar**, click **Configuration > Placement Rules**.
2. Click **+ Create New Rule**.
3. In the **New Placement Rule** window, do the following:
 - a. In the **Rule Name** field, type a name for your new placement rule.
 - b. Select the rule type.
 - c. Complete all required conditions, including deleting or adding conditions as needed, using  and .

Placement Rule conditions

Condition	Explanation	Example
Matches	Performs a literal string match between the key or certificate property and the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Matches <i>server.example.com</i> will match.
Matches Regex	Matches key or certificate property values that match the regular expression pattern specified.	If Subject Alt Name is <i>Server.Example.COM</i> , the condition Subject Alt Name Matches Regex <i>(?i)server.example.com</i> will match.
Starts With	Matches key or certificate property values that start with the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Starts With <i>server</i> will match.

Condition	Explanation	Example
Ends With	Matches key or certificate property values that end with the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Ends With <i>.com</i> will match.
Contains	Matches key or certificate property values that contain the value specified	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Contains <i>example</i> will match.
In	Matches numeric or IP address key or certificate property values that are within the specified range. NOTE Use CIDR notation to specify IP address ranges, or use comma separated values to show multiple IP addresses.	Example 1: If Port is <i>443</i> , the condition Port in <i>0-1024</i> will match. Example 2: If IP address is <i>10.1.0.1</i> , the condition IP Address in ' <i>10.1.0.0/24</i> ' will match, as will IP Address in ' <i>10.1.0.0, 10.1.0.1, 10.1.0.2</i> '.

- d. Select the policy folder into which you want to place keys or certificates that meet the conditions.

This is a required field for SSH keys, and an optional field for certificates.

- e. (Optional) Select the policy folder into which you want to place the certificates' corresponding device.

NOTE For certificates, you must select a policy folder for either the certificate, or the device (or both). You cannot leave both fields blank.

4. Select the folder into which you want to put the placement rule.

NOTE You must have the correct permissions in order to see the folder. See [Permissions overview](#).

IMPORTANT If the folder does not exist when the placement rule is run, the folder will be created and the certificates and devices will be placed in that new folder. This could happen, for example, if you renamed a policy in the Policy Tree, and the corresponding folder no longer existed in the main interface.

5. Add new rules as needed, clicking **+ Create New Rule** and **Save** for each one.

When you're done creating rules, your placement rules should look similar to this:

Name	Rule Type	Certificate Placement	Device/Application Placement
Rule 1	SSH		Policy/Policy A
Rule 2	SSH		Policy/New Policy
Rule 3 cert	Certificate	Policy/New Cert Policy	Policy/New Cert Policy
Rule 0	Certificate	Policy/New Cert Policy	Policy/New Cert Policy
Rule 4	SSH		Policy/New Policy

DID YOU KNOW? You can reorder existing rules by clicking and dragging them up and down the list. Trust Protection Platform executes the rules in the list beginning at the top and moving down. For more information, see ["Editing the order in which placement rules are executed"](#) on page 93.

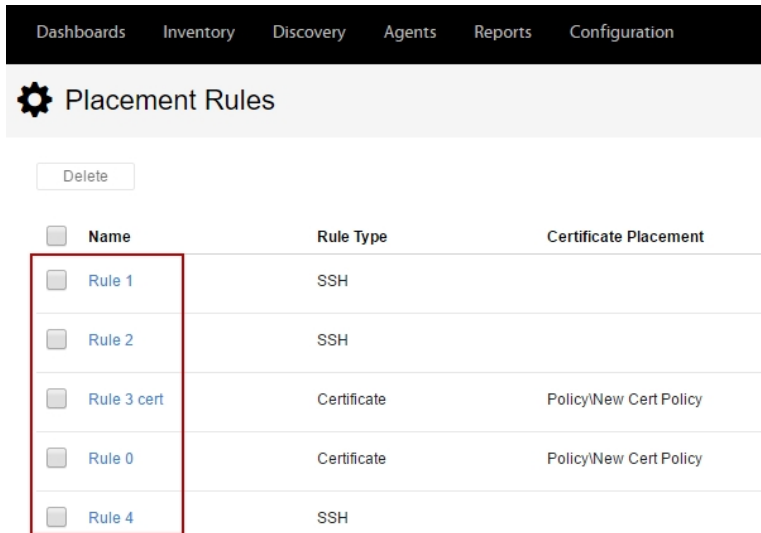
Editing discovery placement rules

You can quickly and easily edit a Discovery placement rule.

DID YOU KNOW? You can reorder existing rules by clicking and dragging them up and down the list. Trust Protection Platform executes the rules in the list beginning at the top and moving down. For more information, see ["Editing the order in which placement rules are executed"](#) on page 93.

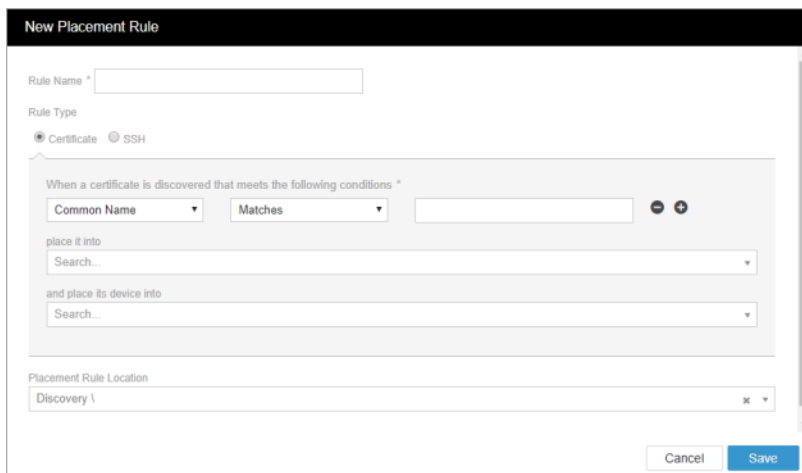
To edit a placement rule

1. From the TLS Protect menu bar, click **Configuration > Placement Rules**.
2. Click the existing placement rule you want to edit.



☐	Name	Rule Type	Certificate Placement
☐	Rule 1	SSH	
☐	Rule 2	SSH	
☐	Rule 3 cert	Certificate	Policy\New Cert Policy
☐	Rule 0	Certificate	Policy\New Cert Policy
☐	Rule 4	SSH	

3. Make changes as needed.



New Placement Rule

Rule Name *

Rule Type

☒ Certificate ☐ SSH

When a certificate is discovered that meets the following conditions *

Common Name ▼ Matches ▼

place it into

Search...

and place its device into

Search...

Placement Rule Location

Discovery \

Cancel Save

4. Click **Save** to save your changes.

Placement Rule conditions

Condition	Explanation	Example
Matches	Performs a literal string match between the key or certificate property and the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Matches <i>server.example.com</i> will match.
Matches Regex	Matches key or certificate property values that match the regular expression pattern specified.	If Subject Alt Name is <i>Server.Example.COM</i> , the condition Subject Alt Name Matches Regex <i>(?i)server.example.com</i> will match.
Starts With	Matches key or certificate property values that start with the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Starts With <i>server</i> will match.
Ends With	Matches key or certificate property values that end with the value specified.	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Ends With <i>.com</i> will match.
Contains	Matches key or certificate property values that contain the value specified	If Subject Alt Name is <i>server.example.com</i> , the condition Subject Alt Name Contains <i>example</i> will match.
In	Matches numeric or IP address key or certificate property values that are within the specified range.	Example 1: If Port is <i>443</i>, the condition Port in <i>0-1024</i> will match. Example 2: If IP address is <i>10.1.0.1</i>, the condition IP Address in '<i>10.1.0.0/24</i>' will match, as will <code>IP Address in '10.1.0.0,10.1.0.1,10.1.0.2'</code>.

NOTE Use CIDR notation to specify IP address ranges, or use comma separated values to show multiple IP addresses.

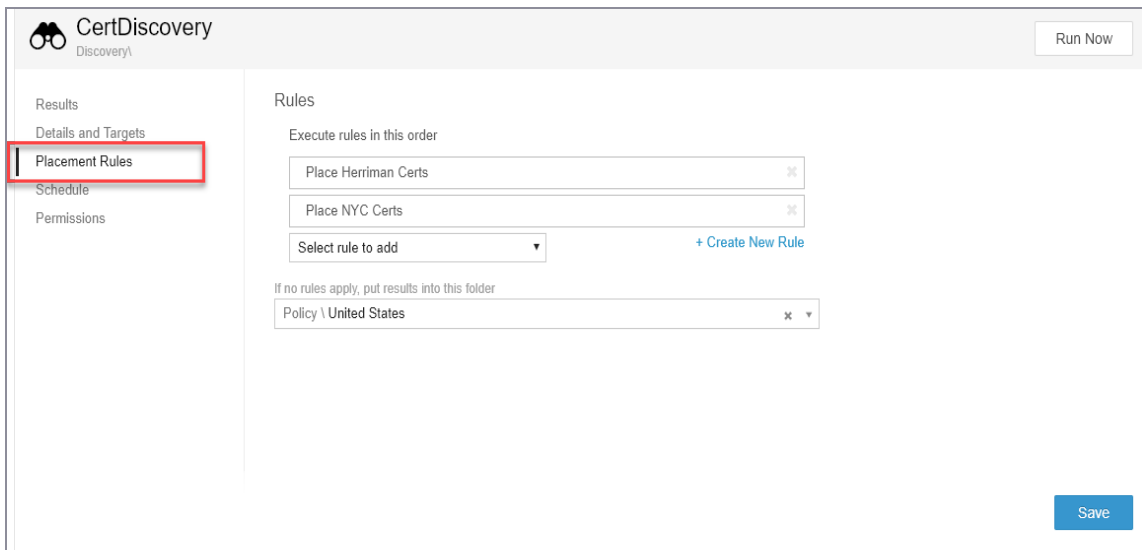
Editing the order in which placement rules are executed

You can reorder placement rules for a specific discovery job so that the rules run the order you specify. Trust Protection Platform executes the rules from the first rule at the top of the list to the last rule at the bottom.

TIP You can create placement rules and use those rules when you create a discovery job. To learn more, see "Creating placement rules" on page 87.

To change the run order of Placement Rules

1. From the **TLS Protect** menu bar, click **Configuration > Placement Rules**.



The screenshot shows the CertDiscovery web interface. On the left, a sidebar contains a menu with options: Results, Details and Targets, Placement Rules (highlighted with a red box), Schedule, and Permissions. The main content area is titled 'Rules' and contains the following elements: a 'Run Now' button in the top right corner; the text 'Execute rules in this order' above a list of two rules, 'Place Herriman Certs' and 'Place NYC Certs', each with a drag handle icon; a 'Select rule to add' dropdown menu and a '+ Create New Rule' link; the text 'If no rules apply, put results into this folder' above a text box containing 'Policy \ United States' with a clear (x) and dropdown (v) icon; and a 'Save' button in the bottom right corner.

2. Drag and drop rules to change their run order.

DID YOU KNOW? When a certificate is discovered, as soon as a valid rule is encountered, that rule is acted on. Then, when the next certificate is discovered, rule processing starts again at the top of the list until a valid rule is encountered. The certificate is placed and the process is repeated until all certificates have been placed.

3. When you're done, click **Save**.

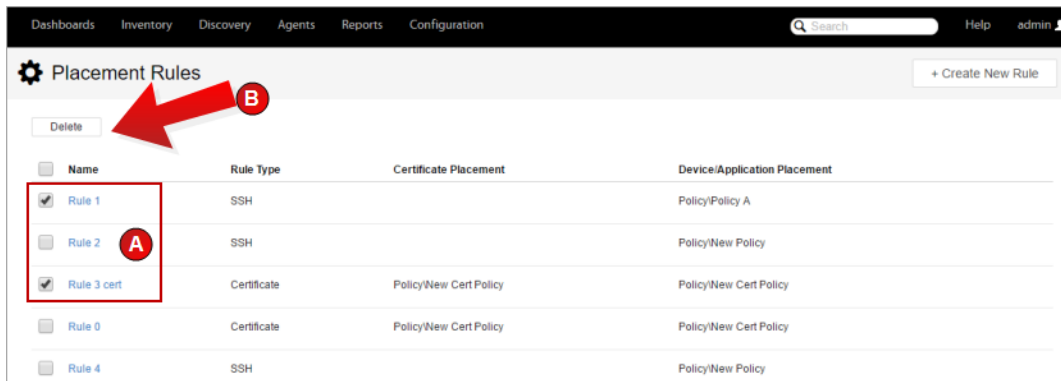
DID YOU KNOW? As Discovery runs, certificate work is processed in batches. As a batch of results is returned, the certificates are placed immediately while Discovery continues working on the next batch. Thus, for large discovery jobs you may see the results of placement while the job is still running. This is expected.

Deleting a network discovery placement rule

If you no longer need to use one or more network discovery placement rules, you can select and delete them from the Placement Rules page.

To delete a placement rule

1. From the [TLS Protect menu bar](#), click **Configuration > Placement Rules**.
2. In the Placement Rules list, select the box for the rules you want to delete.
3. Click **Delete**.



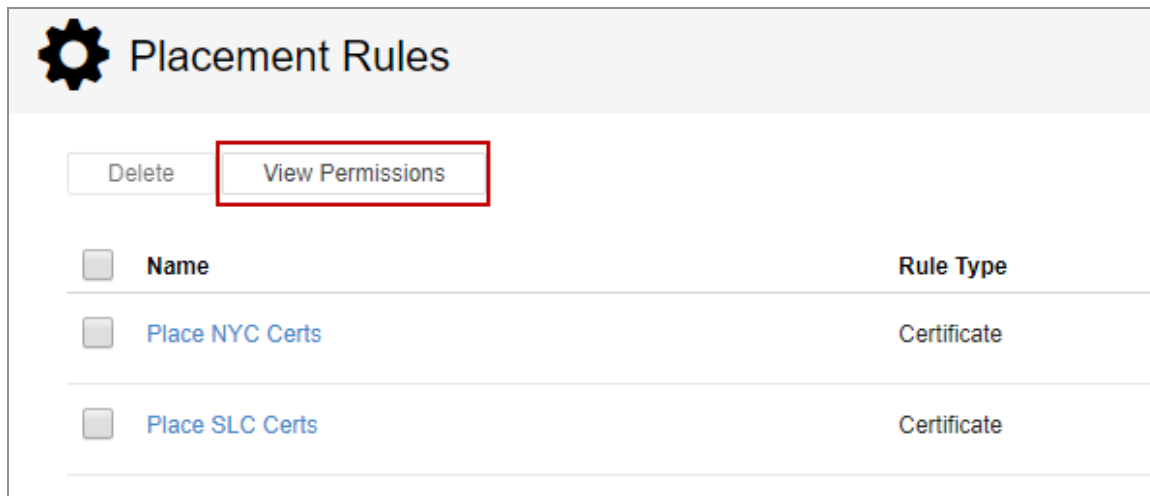
4. In the confirmation window, click **Delete**.

Assigning permissions to placement rules

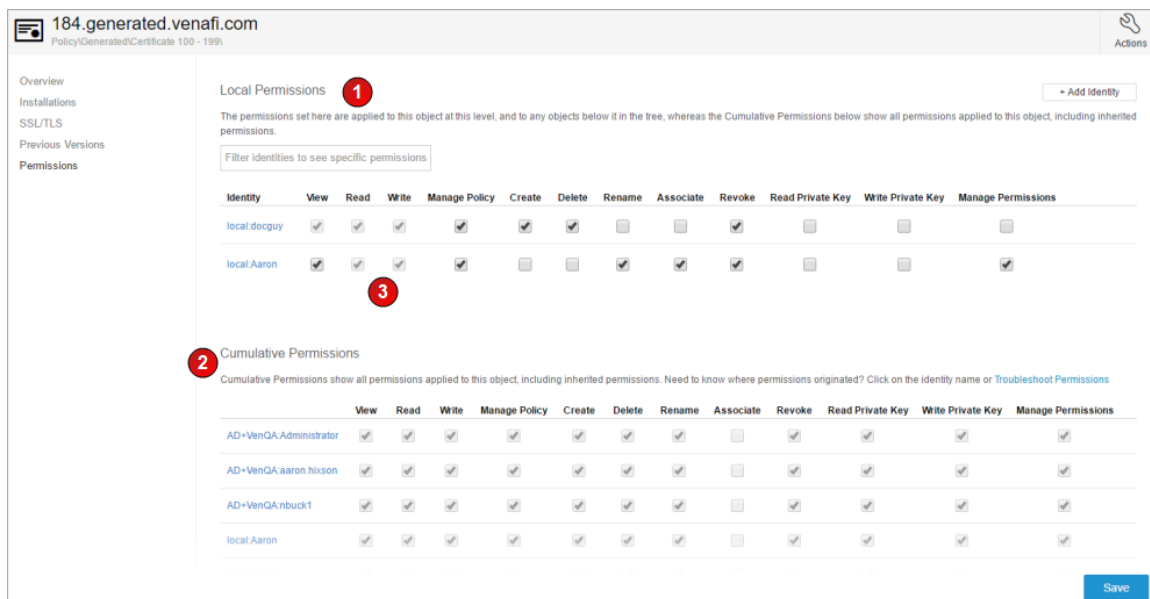
Permissions for placement rules work like permissions for other objects in Aperture.

You assign an identity permission to all placement rules as a group, not to individual placement rules.

To see permissions for placement rules, click the **View Permissions** button at the top of the Placement rules screen:



How Permissions Work in Aperture



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 in Aperture](#).

Certificate and Device Placement jobs

Certificate and Device Placement jobs allow you to organize your certificate and device inventory by applying rules that allow you to filter certificates and devices into specific folders in your system. You can run these rules once, or you can set up a schedule to run these rules on a regular basis.

NOTE This feature works in a way that is similar to applying filters to your email. Once you create the filter in your email program, you have the option to apply the filter to all existing items in your email box. With Certificate and Device Placement jobs, you can also schedule this "filter" to run on a scheduled basis.

This feature allows you to search the inventory for duplicate certificates, and then group the certificates into a single certificate object. When a placement job finds a duplicate certificate, it uses the most recent version (based on date issued) of the certificate as the current version, and moves the duplicate certificate into that certificate's **Previous Versions** tab for certificate history tracking.

Creating a placement job is like creating any other type of job in the Jobs list, you use the **Create New Job** wizard to walk you through the process.

IMPORTANT Placement Jobs only run on Venafi servers that have the **Automatic Layout Manager** installed and enabled in the Venafi Configuration Console. For example, this allows you to have one server in a cluster that processes placement jobs without impacting performance on other servers in the cluster. If Automatic Layout Manager is installed, you can enable or disable it from either the Venafi Configuration Console or from Policy Tree on the Platforms tree.

Creating Certificate and Device Placement jobs

Use this topic for information on how to create Certificate and Device Placement jobs

To create a new Certificate and Device Placement job

1. From the [TLS Protect](#) menu bar, click **Configuration > Jobs**.

(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See ["Filtering the Jobs list by job type"](#) on page 104.

2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Certificate and Device Placement**, and then click **Start**.
4. In the **Details** window, provide information about the placement job you are creating.
 1. **Job Name** (Required). The name of the job that is displayed on the Jobs list.
 2. **Description**. A short description that tells you and others why this placement job was created and what its purpose is.
 3. **Contacts**. One or more people who have information about this job or responsibility for its administration.
 4. **Folders to Scan** (Required). A list of folders that you want to scan as part of this placement job.
 5. **Include Subfolders**. If you want to scan all subfolders of the specified folders, select this check box.
5. Click **Next**.
6. In the **Placement** window, provide information about how certificates and devices should be matched and placed.
 - **Execute Rules in this order** (required). Select a rule that you want to use.
 - Add multiple rules, as needed, if desired by continuing to select the rules. Rules will be processed from top to bottom.
7. If the rule you want to use doesn't exist yet, use the **+Create New Rule** link to create a new placement rule.

For more information on creating new placement rules, see ["Creating placement rules" on page 87](#).
8. If you want to move all certificates and devices for which no rule applies, use the last box, **If no rules apply, put results into this folder**, to specify the location where these certificates and devices should be placed.

If you don't specify a folder here, then certificates and devices that don't match any of the selected rules will remain in the folder where they were found.
9. If you want to **Combine older and newer versions of the same certificate**, select the check box.

For more information about the implications and process of combining certificates during placement, see ["About combining duplicate certificates during placement" on page 101](#).
10. If you want to run the job now, click **Create and Run**.

11. If you just want to create the job now and run it later, click **Create Job**.

You can run the job later, or set up a schedule for it after it is created. To do so, click the job in the Jobs list, then click the **Schedule** tab.

IMPORTANT Placement Jobs only run on Venafi servers that have the **Automatic Layout Manager** installed and enabled in the Venafi Configuration Console. For example, this allows you to have one server in a cluster that processes placement jobs without impacting performance on other servers in the cluster. If Automatic Layout Manager is installed, you can enable or disable it from either the Venafi Configuration Console or from Policy Tree on the Platforms tree.

Viewing and editing Certificate and Device Placement jobs

You can view a placement job's details, as well as schedule the job to run on a regular basis on the Certificate and Device Placement jobs details page.

To view or edit Certificate and Device Placement job details

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
2. (Optional) If you want to filter the list to only see placement jobs, select **Certificate and Device Placement** using the **Job Type** filter.

For more information, see ["Filtering the Jobs list by job type" on page 104](#).

3. From the **Jobs** list, click the job's name.
4. Use the tabs on the left to see additional information, or to edit other parts of the job.

Certificate and Device Placement job details

Placement job details are grouped to make it easier for you to find and analyze relevant information. Use the tabs on the left to switch between sections. The sections on a placement job's details page are:

- Results
- Details and Targets
- Placement Rules
- Schedule
- Permissions

Results

The placement job's **Results** page shows you information about that last time the placement job was run. You can see:

- Status
- Next run
- Last run
- Discovery progress
- Total run time
- Certificates
- Certificate locations
- SSH servers

You have the ability to **Download results** for Certificates and SSH servers in individual CSV files. Be aware that the CSV files may include older results. You can work around this by creating a new scan or by filtering on the **lastsurveyed** column (in the CSV) to see which results are the newest.

Details and Targets

The placement job's **Details** page shows you information about the job. You can edit any of this information, except for the job name. The fields are:

- **Job Name** (Required). The name of the job that is displayed on the Jobs list.
- **Description**. A short description that tells you and others why this placement job was created and what its purpose is.
- **Contacts**. One or more people who have information about this job or responsibility for its administration.
- **Folders to Scan** (Required). A list of folders that you want to scan as part of this placement job.
- **Include Subfolders**. If you want to scan all subfolders of the specified folders, select this check box.

Placement Rules

The placement job's **Placement Rules** page provides details about how certificates and devices are matched and placed.

The **Execute Rules in this order** list shows you the placement rules that have been selected, and the order in which they are run.

- To add an existing placement rule to this placement job, select a rule that you want to use.
- To reorder rules, hold the placement rules and drag them into a different order in the list.
- If the rule you want doesn't exist yet, use the **+Create New Rule** link to create a new placement rule.
- For all certificates and devices for which no rule applies, specify the location where these certificates and devices will be placed.

For more information on creating new placement rules, see ["Creating placement rules" on page 87](#).

Schedule

The placement job's **Schedule** page allows you to determine when the placement job should be run on a regular basis. The default is **Manually**, which means no schedule is set.

To set a schedule

1. In the Frequency field, select the check box and select one of the frequency options:
 - Every Week
 - Every Month
 - Every Year
2. If you selected **Every Week** or **Every Month**, use the following configuration options:
 - Use the **On Days** box to select which days of the week or month you want the job to run.

When you click an option, it is added to the box as a selected option. Click the box again to add multiple values.
 - Use the **Start Time** box to specify what time of day you want the job to run.
3. If you selected **Every Year**, use the following configuration options:

- Use the **Month** and **Day** selectors to pick the date that you want the job to run.
- To add additional dates on which the job should be run, click **+**.
- To remove a date, click **-**.
- Use the **Start Time** box to specify what time of day you want the job to run.

IMPORTANT Placement Jobs only run on Venafi servers that have the **Automatic Layout Manager** installed and enabled in the Venafi Configuration Console. For example, this allows you to have one server in a cluster that processes placement jobs without impacting performance on other servers in the cluster. If Automatic Layout Manager is installed, you can enable or disable it from either the Venafi Configuration Console or from Policy Tree on the Platforms tree.

Permissions

The placement job's **Permissions** page shows what permissions have been granted to this placement job. Permissions for placement jobs work like permissions in all other areas. For details on how to set permissions on objects in, see [About permissions](#) in the Administration Guide.

About combining duplicate certificates during placement

When you are creating or editing a Certificate and Device Placement job, you have the option to **Combine older and newer versions of the same certificate**.

If left unchecked, if there are duplicate certificates in your inventory, they will not be combined, possibly resulting in two of the same certificates existing in different places in your folder structure.

However, if you check the box, you should be aware of the following behavior:

- For every certificate that is evaluated based on the placement rules specified:
 - If Trust Protection Platform determines that the certificate should be moved, then the system scans the entire certificate inventory, looking to see if there is a duplicate certificate.
 - If Trust Protection Platform determines that a certificate does *not* match the placement rules and should not be moved, then the system also does not check for duplicates.
 - If a default folder was selected (you entered something into the **If no rules apply, put results into this folder** field) and Trust Protection Platform determines that a certificate does *not* match the placement rules, it will treat the certificate as if it is being moved, and will scan the entire certificate inventory, looking to see if there is a duplicate certificate.

- If a duplicate certificate is found, the certificates will be combined. The newer version (based on valid from date) will become the main certificate. The older version will be placed in the Previous Versions tab of the certificate details screen for the newer certificate. For specific matching requirements for certificate duplication, see ["About placement of duplicate certificates" on page 111](#).
- The certificate will be placed in the location where the duplicate was found, regardless of where it is in the folder structure. This means, that the placement rules for this certificate will be ignored.

The reason the placement rules are ignored is because at some point a person decided that the certificate belonged in a specific location in your folder structure. We treat the Certificate and Device Placement job as if it is processing an inbox of new certificates and devices, and trying to figure out where to place them in your folder structure. Since a certificate already exists that has been explicitly placed in a location in your tree, we will assume that is the correct location for that certificate, regardless of any placement rules to the contrary in the job.

Thus, the current certificate's location trumps the placement rules in determining where to place a duplicate certificate.

- When a certificate is combined the following happens:
 - All current and historical versions of both certificates are combined in the newer certificate.
 - All associated certificate installations of both certificates are combined in the newer certificate.
- The following items are NOT combined; they are retained from the existing certificate that was found, which is the location where the combined certificate will be placed:
 - Permissions
 - Policy values
 - Renewal values

If you need to move the duplicate certificate as well, you can create a new placement job that scans the location of the duplicate certificate, matches that certificate, and uses a placement job to move that certificate to a different folder.

In general it is a good practice to combine different versions of a certificate, and enabling this setting is recommended by Venafi. Certificate and Device Placement job deduplication is similar to the reconciliation done automatically for Network Discovery, Agent Discovery, and other discovery methods.

However, sometimes combining may not be desirable if your PKI is architected to intentionally have different certificates with the same Common Name, Subject, and Subject Alternative Names. For example, some organizations will intentionally have different *www.example.com* certificates for their load balancers and application servers. If this is the case for your organization, then you do not want to enable combining.

Managing discovery jobs

The Jobs list displays jobs by their job names and sorts them by Job Name (by default). You can change the sort order by clicking any of the column headers that contain ▼ next to the column header.

When you submit a discovery job, the normal flow is *Pending Submission*, *Pending Execution*, sometimes *Waiting for next Execution Window*, *Running*, and *Complete*. The *Complete* status occurs after the todo is done. If discovery job is aborted, the status goes to *Scan Complete (Aborted)*.

TIP To filter the Jobs list by one or more specific job types, use the Job Type filter. For more information, see ["Filtering the Jobs list by job type" on the next page](#).

Column	Sortable?	Description
Job Name	Yes	The name of the job. This field is a link you can click on to view detailed information about this job.
Description	No	A description of the job, if one was added to the job's description field when the job was created. This can be edited by clicking the job name, clicking the Details and Targets tab on the left, and then editing the Description field.
Next Run	Yes	Shows whether a job is set to run manually or at a specific date and time.
Last Run	Yes	Shows a date and time stamp when the job last ran. It doesn't matter if it was done manually or on a schedule.
Type	Yes	Identifies the type of each job (Network Discovery, Onboard Discovery, Bulk Provisioning, or Placement).
Use one of the available filters to quickly limit items in the list according to job types. See "Filtering the Jobs list by job type" on the next page .		

Column	Sortable?	Description
Results	No	Displays the number of certificates found for both Network Discovery and Onboard Discovery jobs. If you have the SSH component installed, Network Discovery jobs can also show the number of discovered SSH servers.
Status	Yes	Displays one of the following values: <i>Aborted</i>, <i>Canceled</i>, <i>Paused</i>, <i>Pending</i>, <i>Pending Execution (internal)</i>, <i>Pending Import</i>, <i>Pending Submission</i>, <i>Running</i>, <i>Complete</i>, <i>Scan Complete (Aborted)</i>, <i>Waiting for next Execution Window</i>. For Network Discovery jobs, a <i>Waiting for next Execution Window</i> status indicates that a job started and then suspended because it encountered a blackout window. For more details about Network Discovery Job blackout windows, see "Scheduling a job" on the facing page.
Priority	Yes	Applies only to Network Discovery and shows the order in which each job will be processed if they are running at the same time. To learn more about changing job priorities, see "Prioritizing network discovery jobs" on page 106 .

Filtering the Jobs list by job type

You can filter your Jobs list using quick filters. For example, if you want to filter the list to show existing Onboard Discovery and Certificate and Device Placement jobs only, click Job Type in the Job Filters and select **Onboard Discovery** and **Certificate and Device Placement**.

For a complete list of available job types, see ["Managing discovery jobs" on the previous page](#).

The screenshot shows the Venafi Jobs management interface. On the left, the 'Jobs Filters' panel is open, with 'Job Type' selected. Under 'Job Type', 'Bulk Provisioning' and 'Onboard Discovery' are selected. The main table displays a list of jobs with columns: Job Name, Status, Next Run, Last Run, Type, Results, and Priority. The 'Type' column is highlighted with a red box, showing 'Bulk Provisioning' for the first two jobs and 'Onboard Discovery' for the last two. The 'Results' column shows certificate counts for each job.

Job Name	Status	Next Run	Last Run	Type	Results	Priority
MyBulkProvisioningJob001	Manual	Never		Bulk Provisioning	Certificates To Provision: 0 Provisioned Certificates via Full Run: 0 Provisioned Certificates via Express Run: 0	Run Now
MyBulkProvisioningJob002	Manual	Never		Bulk Provisioning	Certificates To Provision: 0 Provisioned Certificates via Full Run: 0 Provisioned Certificates via Express Run: 0	Run Now
MyScan	Manual	Never		Onboard Discovery FS LTM Advanced	Certificates: 0	Run Now
dw-OnboardDisco-CAP1	Canceled	Manual	Never	Onboard Discovery CAP1 (SS Settings)	Certificates: 0	Run Now

Scheduling a job

You can schedule a job to run automatically based on your time preferences.

To schedule a job

1. From the Aperture menu bar, click **Configuration > Jobs**.
2. In the Jobs list, click the job you want to schedule.
3. In the sidebar, click **Schedule**, and then do the following:
4. (Optional) If you don't want to set a recurring time to run the job, leave **Frequency** set to **Manually**.
5. If you want to set a recurring time, use the drop-down arrow to select the **Frequency**.

Run Time

Frequency *

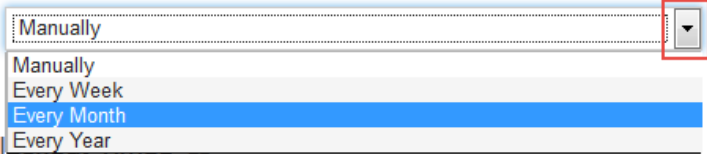
Manually

Manually

Every Week

Every Month

Every Year



6. Set **Timezone** for the job's start time. Consider the following:
 - The **Convert to UTC (default)** option uses your browser's timezone offset to save the start time in UTC format. In this case, Daylight Saving Time (DST) adjustments are not considered.
 - Timezones are assigned per job.
 - On the **Job List** page, times are shown converted to the browser's timezone.
 - Only standard timezones are shown, not separate daylight saving time zones. The timezones that support DST will adjust automatically.
 - There is a potential issue with timezone support on different Windows versions. Newer Windows versions may have updated timezones that older versions cannot parse correctly. This could lead to scheduling issues. It is recommended to have consistent OS versions across TPP servers.
7. As needed, use the **On Days** fields to specify exact dates.
8. Set the **Start Time**, as needed.

9. (Conditional) Set **Blackout Times** by clicking to block out one hour blocks of time to disable processing for those hours. This defines a period of time when the job is prohibited from running, even if the schedule indicates it should run.

Note that the **Blackout Times** feature is works with network discovery job types only.

10. When you're done, click **Save**.

Prioritizing network discovery jobs

For network discovery jobs that are running at the same time (either through scheduling or when run manually) you can configure Trust Protection Platform to run them according to the priority order you specify.

DID YOU KNOW? Network Discovery jobs are the only job types that can be prioritized. This is because Network Discovery jobs can sometimes span multiple days on a single run, and other job types are designed to be completed much faster, typically within a few minutes or hours.

To prioritize the order in which your discovery jobs should run

1. From the **TLS Protect** menu bar, click **Configuration > Jobs**.
2. Click **Change Job Priority**.

The list of job is filtered to the type of jobs that can be prioritized, which is Network Discovery jobs.

3. Drag a job name to move it up or down in the list .

The Priority column does not update until you save your work, so that you can see the original priority order before you made your changes.

4. When you are finished prioritizing, click **Done**.

The priority order of Network Discovery jobs is updated and can be seen in the Jobs list.

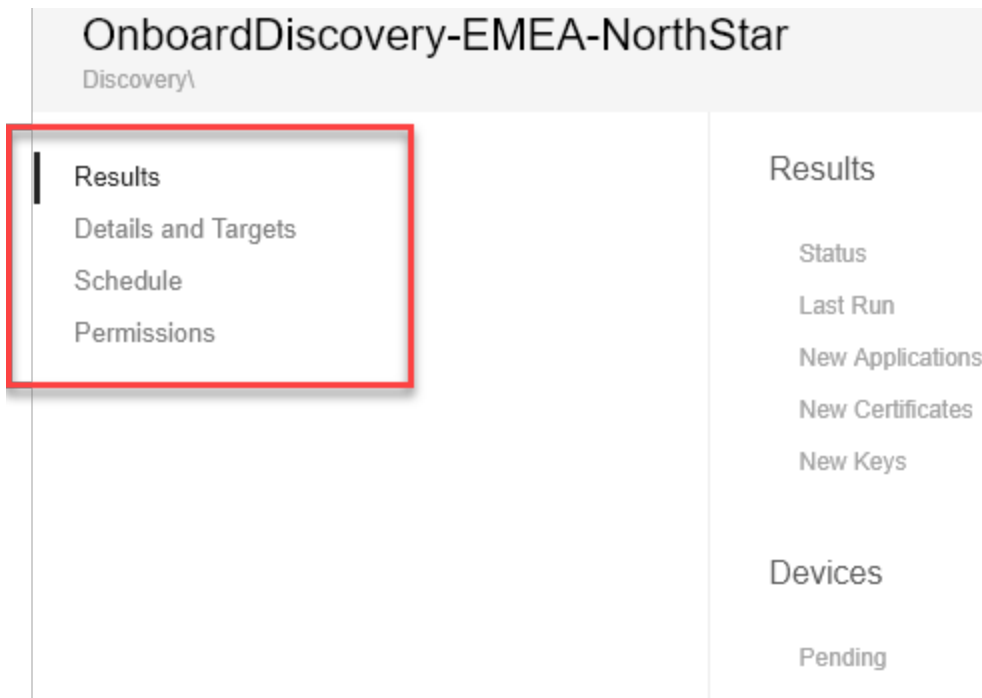
Editing job settings

If you need to change the settings for existing discovery jobs, you can edit and apply the settings in Jobs.

To edit a Job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
2. In the **Job Name** column, click the job that you want to edit.
3. On the job's Details page, use the sidebar to modify settings.

For example, if you're editing an onboard discovery job, settings are found on the left sidebar:



4. When you finish making changes, click **Save**.

Renaming a job

You can edit the name of any existing job type. This can be helpful when you discover that an existing name is not descriptive or meaningful enough to other users.

To rename a job

NOTE You need the **rename** permission to the job, or this functionality won't be available to you.

1. From the SSH Protect menu bar, click **Configuration > Jobs** .
2. Locate the job you want to change.
3. Click on the job name to open the details page.
4. Hover your mouse pointer over the job name until you see the name highlighted, and then click it.
5. In the **Rename** box, type the new name in the **New Name** field, and then click **OK**.

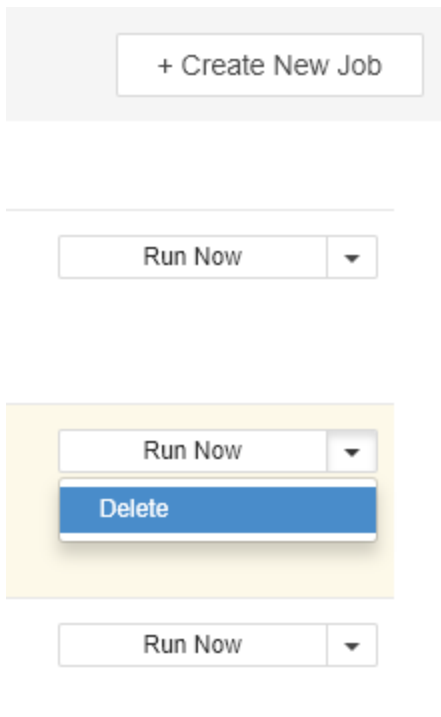
Object names may not contain the backslash (\) or less-than sign (<) characters. Object names (including their path ancestors in the policy tree) must be fewer than 255 total characters.

Deleting jobs

If you no longer need a particular job, you can delete it using the Quick Action list.

To delete a job

1. From the Aperture menu bar, click **Configuration > Jobs**.
2. In the **Discovery** jobs list, find the job you want to delete, and then in the far right column, click **Delete** from the **Quick Action** list.



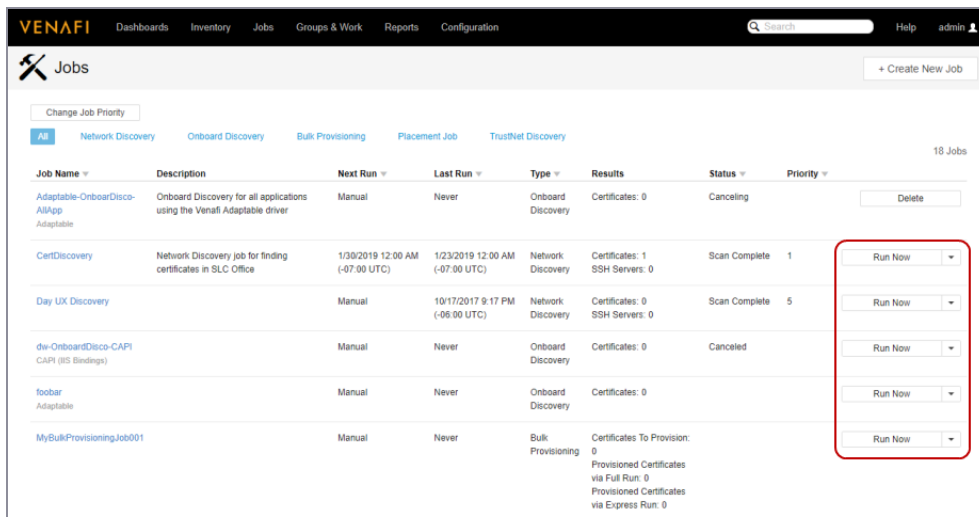
3. In the confirmation window, click **Delete**.

Running a job manually

You can run a job manually if you want to perform the job function between scheduled jobs.

To run a job manually

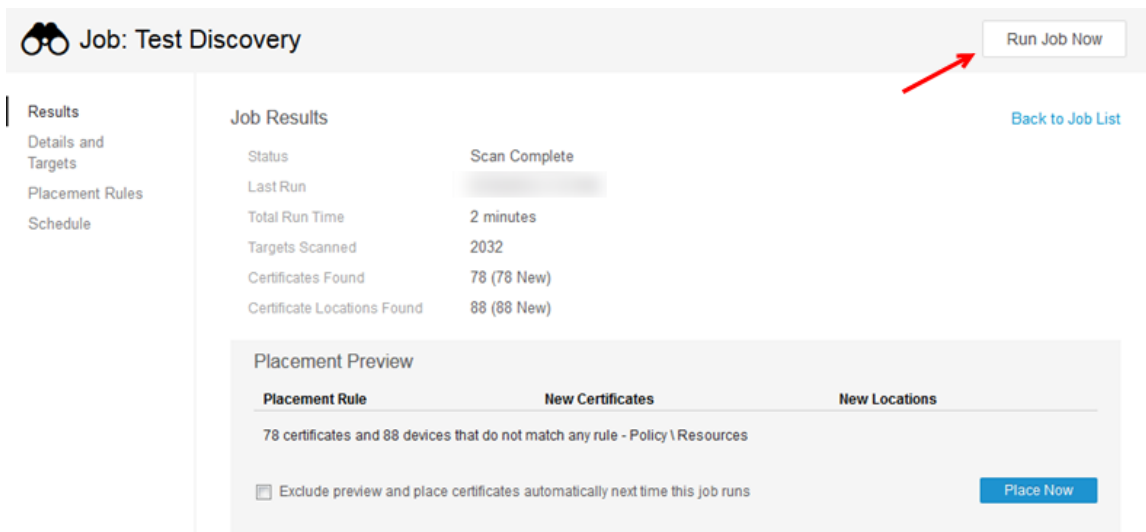
1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
2. In the Jobs list, find the job you want to run, and then click **Run Now** from the Quick Action list.



Job Name	Description	Next Run	Last Run	Type	Results	Status	Priority
Adaptable-OnboardDisco-AllApp	Onboard Discovery for all applications using the Venafi Adaptable driver	Manual	Never	Onboard Discovery	Certificates: 0	Canceling	
CertDiscovery	Network Discovery job for finding certificates in SLC Office	1/30/2019 12:00 AM (-07:00 UTC)	1/23/2019 12:00 AM (-07:00 UTC)	Network Discovery	Certificates: 1 SSH Servers: 0	Scan Complete	1
Day UX Discovery		Manual	10/17/2017 9:17 PM (-06:00 UTC)	Network Discovery	Certificates: 0 SSH Servers: 0	Scan Complete	5
dev-OnboardDisco-CAPI	CAPI (IS Bindings)	Manual	Never	Onboard Discovery	Certificates: 0	Canceled	
foobar	Adaptable	Manual	Never	Onboard Discovery	Certificates: 0		
MyBulkProvisioningJob001		Manual	Never	Bulk Provisioning	Certificates To Provision: 0 Provisioned Certificates via Full Run: 0 Provisioned Certificates via Express Run: 0		

OR

From a job's detail page, click **Run Job**.



Job: Test Discovery Run Job Now

[Back to Job List](#)

Results

- Details and Targets
- Placement Rules
- Schedule

Job Results

Status: Scan Complete

Last Run: [Progress Bar]

Total Run Time: 2 minutes

Targets Scanned: 2032

Certificates Found: 78 (78 New)

Certificate Locations Found: 88 (88 New)

Placement Preview

Placement Rule	New Certificates	New Locations
78 certificates and 88 devices that do not match any rule - Policy\Resources		

☐ Exclude preview and place certificates automatically next time this job runs

Place Now

Manually running, canceling, or pausing a discovery job

When you start a discover job manually, it runs under the same execution schedule as a scheduled discovery.

NOTE You must have the *View* and *Write* permissions to the discovery object.

TIP You can also run a quick discovery of a specific IP address using the classic policy tree. For more information, see ["Using Instant Discovery" on page 83](#).

To manually run, abort, or pause a discovery job

1. On the menu, click **Configuration > Jobs**.
2. In the **Jobs** list, click the job name you want to run.
3. To run the discovery, click **Run Now**.

After you click **Run Now**, the button changes to **Cancel** so you can stop the scan if needed.

4. To pause the discovery currently in progress, click **Pause**.

The pause may not be immediate. The discovery job completes the current block of addresses it is scanning before pausing the entire discovery operation.

5. To resume the currently paused discovery, click **Resume**.

About placement of duplicate certificates

When discovery finds a new version of an existing certificate on another device, TLS Protect combines the certificates, placing the older certificate in the certificate history of the newer certificate.

EXAMPLE Suppose you have a certificate created on 01/01/2021, and the certificate was installed on device A and placed in a policy folder called *SouthAmerica*. Suppose that certificate was renewed on 01/01/2022, and the renewed certificate was subsequently discovered on device B (but the older version was still on device A).

In this case, TLS Protect will combine the certificates in the *SouthAmerica* folder, with the version from device A (the 2021 version of the certificate) in the history of the version from device B (the 2022 version of the certificate).

At the end of the discovery process, there will be a single certificate stored in the *SouthAmerica* folder.

When validation is attempted for device B, validation is successful, since device B has the newer version of the certificate. When validation is attempted for device A, validation fails, because device A has the older version of the certificate, which is now a historical certificate. Simply deploy the new certificate to device A, and the issue is resolved.

How does TLS Protect determine if a certificate is a duplicate?

TLS Protect uses the following criteria to reconcile certificates that are already under management:

- The **subject**, **key usage**, and **enhanced key usages** are all identical.
- The **SAN** information is similar enough for a match, which means:
 - 4 SAN DNS entries must match.
 - If there are 1 to 4 SAN DNS entries on the certificate, all must match.
 - If more than 4 SAN DNS entries are found, then 50% or more of them must match (e.g. if 5 SAN entries are found, 3 must match).

Any certificates that *match all of the criteria* are deemed *related*.

For choosing historical placement of *related* certificates, Trust Protection Platform looks at the **Valid To** or **Not After** certificate properties to determine which of the certificates is *newer*.

Moving certificates and keys in bulk after Discovery

After a discovery job is complete and certificates and keys have been placed, you may want to move items in bulk from one policy to another. This is especially helpful when moving certificates or keys from the default policy to their correct folders.

To move multiple certificates or keys at the same time (bulk move)

1. From the menu, open the correct inventory.
2. Select the items you want to move . You can use the filters to help you refine the list.
3. **Tip:** If you want to move all of the visible items, select the checkbox next to **Nickname**.

Move to ... 100 certificate(s) selected.

Select all visible items in results list

	Nickname	Installations	Valid To	Risks	Issuer
☒	101.generated.venafi.com	1	12/19/2017	Failed Validation, No Owner Assigned, Unapproved Issuer	Google In
☒	102.generated.venafi.com	23	1/7/2019	Failed Validation, No Owner Assigned, Unapproved Issuer	QA Venafi
☒	103.generated.venafi.com	2	11/14/2018	Failed Validation, No Owner Assigned, Unapproved Issuer	QA Venafi
☒	104.generated.venafi.com	0	6/29/2016	No Owner Assigned, Weak Key	Self Signe
☒	105.generated.venafi.com	0	5/5/2018	No Owner Assigned, Unapproved Issuer	GlobalSig GlobalSig
☒	106.generated.venafi.com	0	11/13/2018	No Owner Assigned, Unapproved Issuer	QA Venafi

IMPORTANT The select all box only selects the visible items in the list. Thus, if there are 200 items that match the filter results, but only 100 items are displayed, on the 100 displayed items will be moved. To display more items, scroll to the bottom of the list and click the **Load** banner.

4. When you've selected the items you want to move, click **Move To...**

Move to ... 3 certificate(s) selected.

	Nickname	Installations	Valid To	Risks
☒	101.generated.venafi.com	1	12/19/2017	Failed Validation, No Owner Assigned, Unapproved Issuer
☒	102.generated.venafi.com	23	1/7/2019	Failed Validation, No Owner Assigned, Unapproved Issuer
☒	103.generated.venafi.com	2	11/14/2018	Failed Validation, No Owner Assigned, Unapproved Issuer
☐	104.generated.venafi.com	0	6/29/2016	No Owner Assigned, Weak Key
☒	105.generated.venafi.com	0	5/5/2018	No Owner Assigned, Unapproved Issuer

5. Use the drop-down arrow to choose the new folder.
6. Click OK.

You'll see a confirmation message and a progress bar indicating that items are being moved.

Move Certificates

Moving 3 certificates into Policy\AA Aperture Policies\Policy 5 - Locks that will match CSR . . .

Do not close the window until the process is complete

33% complete

Stop

What if I need to stop the process?

- Move Certificates

Moving 100 certificates into Policy\AA Aperture Policies . . .

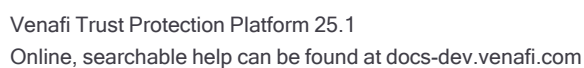
If you stop the process now, not all certificates will be moved. Are you sure you want to do this?

26% complete

No

Yes

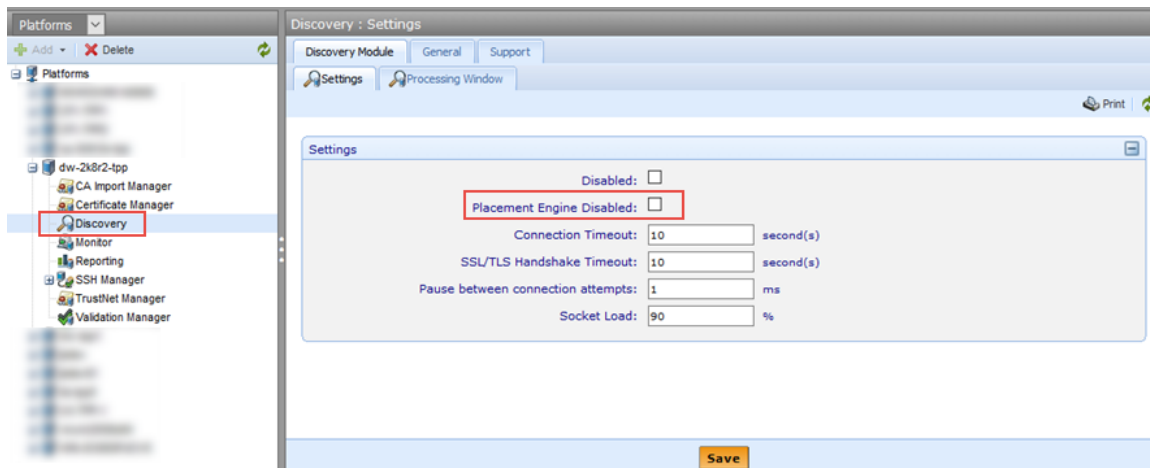
Review the notification that tells you how many certificates or keys were moved before the stop was initiated.



Enabling a discovery placement engine

To enable a discovery placement engine

1. From the **Platform menu bar**, click **Policy Tree**.
2. Find the discovery engine that you want to enable.
3. On the **Settings** tab, clear the **Placement Engine Disabled** checkbox.



Specifying discovery exclusion objects

Exclusion objects define ranges of IPv4 addresses and ports that you do not want the Discovery engine to scan. You can also exclude certificates already being managed in the Policy tree from discovery or exclude certificates from discovery based on the certificate's Issuer or Subject DN.

Exclusion objects are referenced in the Discovery object configuration to apply the exclusions to individual discoveries.

NOTE You must have *view* and *create* permissions to the root Discovery object to create Exclusion objects.

To specify discovery exclusion objects for an existing job

1. Log in to Aperture.
2. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
3. On the **Jobs** page, click the **Job Name** you want to modify.
(Optional) To filter the **Jobs** list to show jobs of only a specific type, click the related job type filter.
4. In the job's page, click **Details and Targets**.

Nightly Discovery

Results

Details and Targets

Placement Rules

Schedule

Permissions

Nightly Discovery

Description

Contacts

Search for an identity

Targets

IP, CIDR, and Hostnames (one per line) *

1.1.1.1

Ports *

1311,18072,18080-18085,18090-18094,1920,2083,2087,2096,22,2211,2484,28080,2949,3268,3269,3414,443-449,465,4712,4843,5223,5358,563,636,6619,6679,6697,695,7002,80,8080,8222,8243,8333,8443,8878,8881,8882,9043,9090,9091,9443,981-995

Exclusions

Search...

5. Under **Targets**, click the **Exclusions** field.
6. Select the exclusions for the discovery job.

NOTE You must create exclusions in order to see them in the list. To learn how to create exclusion objects, see ["Excluding IP addresses and host names from discovery scans"](#) on [page 63](#).

7. When you're done, click **Save**.

3

Importing certificates from a certificate authority

You can import certificates based on the issuing certificate authority (CA). After the import is configured, all certificates issued by a specified CA are identified and then placed into the folders that you specify.

TIP Use a CA import to establish your initial inventory. Importing certificates can help you keep your inventory up-to-date because many of these certificates are enrolled outside of Trust Protection Platform.

Importing certificates lets you

- use Trust Protection Platform to bring certificates issued by their CA under management, replacing processes that are currently manual and require multiple steps
- keep track of certificates that Trust Protection Platform did not enroll

These often include mobile, user, and client device certificates. This gives you visibility over your entire certificate population, not just server certificates.

- automatically reconcile imported certificates with existing certificates to ensure that Trust Protection Platform is tracking current certificates

This chapter contains the following topics:

Importing certificates from an Amazon Private CA.....	118

Importing certificates from a Microsoft CA	120
Importing certificates using the Adaptable CA driver	123
Running a CA import manually	128
CA Import reconciliation rules	129
Verify certificate import results	129
Enable or disable a CA import service module	131

Importing certificates from an Amazon Private CA

You can import certificates issued by an Amazon Private CA by configuring a *Certificate Import* job in Aperture. After the import is configured, all certificates issued by your specified CA are retrieved and placed into folders that you designate.

For additional information, see [Integrating Amazon Certificate Manager with Venafi](#) in the Certificate Authority and Hosting Platform Integration Guide.

NOTE The certificate import feature imports only those certificates that were issued since the last time the import job ran. So this means that for a *new import job*, all certificates previously issued would be imported.

Re-running an import job does not restore certificates that were deleted; Trust Protection Platform assumes that when you delete a certificate, you did so because you don't want it in your inventory (and you also don't want it to be restored every time you run an import job).

Therefore, if you want to restore deleted certificates, you must create and run a new certificate import job.

First things first

Before you create your Private CA certificate import job, review the following prerequisite steps:

- In ACM, verify that the Amazon Private CA you'll be using has been configured to generate audit reports to an S3 bucket. For more information, see [Preparing an Amazon S3 bucket for audit reports](https://docs.aws.amazon.com/acm-pca/latest/userguide/PcaAuditReport.html) (<https://docs.aws.amazon.com/acm-pca/latest/userguide/PcaAuditReport.html>).
- Make sure you have permissions to the S3 Bucket. If, when configuring your import job, you specify an S3 bucket for which you don't have the required permissions, you'll encounter an error when you run the job.

DID YOU KNOW? Trust Protection Platform generates an audit report into the S3 bucket whenever you run the import job. However, AWS only allows audit reports to be run every 30 minutes. To work around this, Venafi doesn't delete the generated report from the S3 bucket after running the import job, which allows you to run the job again within the 30 minute window.

To create a new Certificate Import job

1. From the **TLS Protect** menu bar, click **Configuration > Jobs**.
(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See ["Filtering the Jobs list by job type" on page 104](#).
2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Certificate Import**, and then click **Start**.
4. On the **Details** panel of the **New Certificate Import Job**, type a name for your new job in the **Job Name** field page.
5. (Optional) In the **Description** field, type a description of 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.
6. From the **Import Type** list, select **Amazon Private CA**.
7. (Optional) In the **Contacts** field, begin typing a user name to specify one or more contacts for your new job, and then click **Next**.
To add multiple contact names, press **Enter** after each name.
8. Click **Next**.
9. On the **Settings** panel, select the Amazon credential that has permissions to the Private CA.
10. From the **Region** list, select the specific region where your Private CA is located.

11. In **S3 Bucket Name**, type the name of the S3 Bucket associated with the Private CA generated audit report, and to which you have the required permissions.

NOTE Make sure you have permissions to the S3 Bucket you specify. Trust Protection Platform finds all available S3 buckets in ACM, even those for which you do not have the required permissions. If you specify an S3 bucket for which you don't have the required permissions, then when you run the import job, you'll eventually encounter an error.

12. From the **Private CA** list, select the private CA, and then click **Retrieve Private CAs and Validate S3 Bucket**.
13. (Optional) Select the **Include Expired Certificates** and/or **Include Revoked Certificates** check boxes if you want them included during the import.
14. Click **Next**.
15. On the **Placement** panel, under **Placement Settings**, select a folder where you want newly found certificates to be placed.

TIP You can create a *Certificate and Device Placement* job to reorganize your certificates automatically after they've been placed in a folder by your certificate import job?

See "[Certificate and Device Placement jobs](#)" on page 96 in the Certificate Management Guide.

16. When you're finished, click **Create Job**.

(Optional) If you want to run the new job immediately, click **Create and Run**. To learn more, see "[Running a CA import manually](#)" on page 128.

Importing certificates from a Microsoft CA

You can import certificates issued by a Microsoft Active Directory Certificate Services certificate authority (CA) by configuring a *Certificate Import* job in Aperture. After the import is configured, all certificates issued by your specified CA are retrieved and placed into folders that you designate.

NOTE The certificate import feature imports only those certificates that were issued since the last time the import job ran. So this means that for a *new import job*, all certificates previously issued would be imported.

Re-running an import job does not restore certificates that were deleted; Trust Protection Platform assumes that when you delete a certificate, you did so because you don't want it in your inventory (and you also don't want it to be restored every time you run an import job).

Therefore, if you want to restore deleted certificates, you must create and run a new certificate import job.

To create a new Certificate Import job

1. From the **TLS Protect** menu bar, click **Configuration > Jobs**.

(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See "[Filtering the Jobs list by job type](#)" on page 104.
2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Certificate Import**, and then click **Start**.
4. On the **Details** panel of the **New Certificate Import Job**, type a name for your new job in the **Job Name** field page.
5. (Optional) In the **Description** field, type a description that can help other administrators better understand the purpose of your new job.

This can be helpful in communicating with other administrators or to remind yourself why you created the new job.
6. From the **Import Type** list, select **Microsoft CA**.
7. (Optional) In the **Contacts** field, begin typing a user name to specify one or more contacts for your new job, and then click **Next**.

To add multiple contact names, press **Enter** after each name.
8. Click **Next**.
9. On the **Settings** panel, specify the **Hostname or IP Address** of the CA you selected.

10. From the **Credentials** list, select the credential that stores the user name and password required to connect to your CA server.

For more information about credential requirements, see [Configuring the Microsoft Active Directory Certificate Services \(ADCS\) - Enterprise and Standalone template object](#).

11. Type a **Service Name**.

The *service name* is the common name (CN) of the CA's certificate. It's also the name of the CA as it appears in the *Certificates* snap-in in the Microsoft Management Console (MMC).

12. Click **Get Templates** to load available CA templates in the **CA Templates Found** list.
13. In the **CA Templates Found** list, select and move one or more templates you want to use to the **Selected for this Import** box.
14. (Optional) Below the **CA Templates Found** box, select the **Include Expired Certificates** and/or **Include Revoked Certificates** check boxes if you want them included during the import.
15. Choose **Use CA Template Name as Certificate Origin** if the template name is meaningful to your team.

OR

Choose **Specify Certificate Origin** if you want to use a custom name.
16. Click **Next**.
17. On the **Placement** panel, under **Placement Settings**, select a folder where you want newly found certificates to be placed.

TIP You can create a *Certificate and Device Placement* job to reorganize your certificates automatically after they've been placed in a folder by your certificate import job?

See "Certificate and Device Placement jobs" on page 96 in the Certificate Management Guide.

18. When you're finished, click **Create Job**.

(Optional) If you want to run the new job immediately, click **Create and Run**. To learn more, see "Running a CA import manually" on page 128.

Importing certificates using the Adaptable CA driver

You can import certificates based on an issuing certificate authority (CA) by configuring a *Certificate Import* job. After the import is configured, all certificates issued by your specified CA are identified and placed into folders that you designate.

NOTE The certificate import feature imports only those certificates that were issued since the last time the import job ran. So this means that for a *new import job*, all certificates previously issued would be imported.

Re-running an import job does not restore certificates that were deleted; Trust Protection Platform assumes that when you delete a certificate, you did so because you don't want it in your inventory (and you also don't want it to be restored every time you run an import job).

Therefore, if you want to restore deleted certificates, you must create and run a new certificate import job.

To create a new Certificate Import job using Adaptable CA

1. From the **TLS Protect** menu bar, click **Configuration > Jobs**.
(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See "[Filtering the Jobs list by job type](#)" on page 104.
2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Certificate Import**, and then click **Start**.
4. On the **Details** panel, in the **Job Name** field of the **New Certificate Import Job** page, type a name for your new job.
5. (Optional) In the **Description** field, type 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.
6. From the **Import Type** list, select **Adaptable**.

7. (Optional) In the **Contacts** field, begin typing a user name to specify one or more contacts for your new job, and then click **Next**.

To add multiple contact names, press **Enter** after finding each name.

8. On the **Settings** page under **Job Settings**, do the following:

- a. From the **PowerShell Script** list, select your Windows PowerShell script.

Only scripts that are contained in the Program Files\Venafi\Scripts\AdaptableCA folder appear in this list. If the script you want to use isn't listed, verify that it has been placed into the correct directory on your Trust Protection Platform server.

For information about creating and modifying Adaptable CA PowerShell scripts, see [About the Adaptable CA PowerShell script](#).

- b. (Optional) If you want to enhance troubleshooting capabilities of your Adaptable CA-enabled Certificate Import jobAdaptable Flow, select the **Enable Debug Logging** check box.

For information about how enabling this option works with the PowerShell script, see [About debug logging](#) in the Adaptable CA Adaptable Flow PowerShell script reference.

- c. (Optional) In **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 ["About automating PowerShell script updates following service URL and configuration changes"](#) on page 126.

- d. (Optional) In **Profile String**, type the profile string used by your PowerShell script.

Specifying a certificate product, profile, or template here lets you use the same script for different types of certificates supported by the target CA.

This setting works with **Service Address** (previous step) 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). Refer to the previous step.

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.

- e. Use **Username Credential** and **Certificate Credential** to select one or both credentials.

TIP If your organization requires two-factor authentication, then specify both credentials.

- f. (Optional)(Conditional) If you need to select another credential, then from the **Secondary Credential** field, select a username, certificate, or password 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.

- g. (Optional) Below the **PowerShell Script** box, select or clear the following check boxes:

- **Include Expired Certificates** and **Include Revoked Certificates**: Select one or both options if you want to include expired and revoked certificates during the import.
- **Assign Contact value to Issued To**: Select this option if you're importing user certificates so you can associate certificates with the correct user identity. You'll likely want to select this option if you're using Venafi Client Protect.

For more information about Client Protect, see [Client Protect Introduction](#) in the *Client Protect Administration Guide*.

- h. In **Certificate Origin**, type in custom text related to the certificate's origin.

This option lets you provide text that can aid your team in tracking certificates and is for reporting purposes only.

9. Click **Next**.

10. On the **Placement** page, under **Placement Settings**, select a folder where you want newly found certificates to be placed.

TIP You can create a *Certificate and Device Placement* job to reorganize your certificates automatically after they've been placed in a folder by your certificate import job.

For more information, see "[Certificate and Device Placement jobs](#)" on page 96 in the Certificate Management Guide.

11. Click **Next**.
12. On the **Occurrence** page, if you want this new job to run at a specific time automatically, use the Frequency list to configure it. specify when you want this new job to run.
13. When you're finished, click **Create Job**.

(Optional) If you want to run the new job immediately, click **Create & Run**.

To learn more, see "[Running a CA import manually](#)" on page 128.

About automating PowerShell script updates following service URL and configuration changes

Beginning with Trust Protection Platform version 20.1, you can configure your Adaptable CACertificate Import jobs with two new settings: **Service Address** and **Profile String**. The primary benefit of these settings is for third-party Venafi partners as they enable partner's PowerShell scripts to be used *as-is* without customers having to customize them. So unless you're developing and testing a PowerShell script, you'll not likely need to ever use these settings.

However, a secondary benefit is that in the event that service URL or configuration changes are made, the values you specify for these settings 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.

What happens to my services if changes are made?

So what happens when changes are made to service URLs (and/or associated configurations) that are referenced by your Adaptable PowerShell scripts? What if your provider makes those changes without your knowledge?

In those cases, you'd have to update every script on all Trust Protection Platform servers where those scripts exist. In addition, you'd have to re-validate each script. This requirement is actually an important Venafi security feature designed to prevent unauthorized changes (see [Protecting against unapproved changes to Adaptable CA scripts](#)).

However, if you configure these settings in your Adaptable CA Certificate Import job, then in the event that changes do occur, those values 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 information about configuring these settings, see ["Importing certificates using the Adaptable CA driver" on page 123](#).

Using sample Adaptable PowerShell scripts

When you install Trust Protection Platform, PowerShell reference samples are included in the `\Venafi\Scripts\AdaptableCA\Samples` folder. You can use the reference samples to better understand how to configure your own scripts.

The reference samples are *fully-functional implementations* that let you accomplish various tasks.

You can use the PEM (*PEM Certificate Import.ps1*) sample script to import certificates and private keys from PEM and PKCS#12 files. For password encrypted private keys and PKCS#12 keystores, the script must return the decryption password along with the key/keystore data if they're to be successfully imported.

You can use the DigiCert (*DigiCert Certificate Import.ps1*) sample script to import certificates from a DigiCert CertCentral account. The DigiCert API has rate limits that constrain the number of certificates that can be imported per hour. The sample script has been designed to import as many certificates as it can while staying far enough below the rate limit to prevent issues with enrolling or revoking DigiCert certificates. Because of this it might take a few hours to import all of the certificates from your DigiCert CertCentral account.

To use the sample scripts

1. Copy the sample script files (.ps1) from the `\Venafi\Scripts\AdaptableCA\Samples` directory to the `\Venafi\Scripts\AdaptableCA` directory.
2. (Conditional) You must also copy the PowerShell script to all Trust Protection Platform servers that are utilized in enrollment, or that are serving up an administration console (e.g. Policy Tree or Aperture).
3. Configure a certificate import job in Aperture and when prompted, select the sample PowerShell script you want to use.

See ["Importing certificates using the Adaptable CA driver" on page 123](#).

When you're ready to customize your own scripts, refer to the [Import-Certificates](#) function in the [PowerShell script reference](#) section of the *Certificate Authority and Hosting Platform Integration Guide*.

Before you begin modifying scripts, review the topic ["Protecting against unapproved changes to Adaptable Bulk Provisioning scripts" on page 524](#).

Running a CA import manually

After you've configured a certificate authority (CA) import job, you can run the import manually at anytime.

To run a job manually

1. From the TLS Protect menu bar, click **Configuration > Jobs**.
2. In the **Jobs** list, highlight the job you want to run, and then click **Run Now** from the Quick Action list.

The screenshot shows the Venafi Jobs page. The top navigation bar includes 'VENAFI', 'Dashboards', 'Inventory', 'Jobs', 'Groups & Work', 'Reports', and 'Configuration'. A search bar and user profile are on the right. The main section is titled 'Jobs' and has a '+ Create New Job' button. Below this is a 'Change Job Priority' dropdown and tabs for 'Network Discovery', 'Onboard Discovery', 'Bulk Provisioning', 'Placement Job', and 'TrustNet Discovery'. A table lists 18 jobs. The 'CertDiscovery' job is highlighted, and its 'Run Now' button is circled in red. Other jobs listed include 'Adaptable-OnboardDisco-AllApp', 'Day UX Discovery', 'dis-OnboardDisco-CAP1', 'foobar', and 'MyBulkProvisioningJob001'.

Job Name	Description	Next Run	Last Run	Type	Results	Status	Priority	Quick Action
Adaptable-OnboardDisco-AllApp	Onboard Discovery for all applications using the Venafi Adaptable driver	Manual	Never	Onboard Discovery	Certificates: 0	Canceling		Delete
CertDiscovery	Network Discovery job for finding certificates in SLC Office	1/30/2019 12:00 AM (-07:00 UTC)	1/23/2019 12:00 AM (-07:00 UTC)	Network Discovery	Certificates: 1 SSH Servers: 0	Scan Complete	1	Run Now
Day UX Discovery		Manual	10/17/2017 9:17 PM (-08:00 UTC)	Network Discovery	Certificates: 0 SSH Servers: 0	Scan Complete	5	Run Now
dis-OnboardDisco-CAP1	CAP1 (SS Bindings)	Manual	Never	Onboard Discovery	Certificates: 0	Canceled		Run Now
foobar	Adaptable	Manual	Never	Onboard Discovery	Certificates: 0			Run Now
MyBulkProvisioningJob001		Manual	Never	Bulk Provisioning	Certificates To Provision: 0 Provisioned Certificates via Full Run: 0 Provisioned Certificates via Express Run: 0			Run Now

OR

From the **Details and Targets** tab of a job, click **Run Now**.

The screenshot shows the 'Job: Test Discovery' details page. The top navigation bar includes 'VENAFI', 'Dashboards', 'Inventory', 'Jobs', 'Groups & Work', 'Reports', and 'Configuration'. A search bar and user profile are on the right. The main section is titled 'Job: Test Discovery' and has a 'Run Job Now' button. Below this is a 'Back to Job List' link. The page is divided into two main sections: 'Results' and 'Job Results'. The 'Results' section has tabs for 'Details and Targets', 'Placement Rules', and 'Schedule'. The 'Job Results' section shows the status 'Scan Complete' and a progress bar. Below this is a table with the following data:

Job Results	Value
Status	Scan Complete
Last Run	
Total Run Time	2 minutes
Targets Scanned	2032
Certificates Found	78 (78 New)
Certificate Locations Found	88 (88 New)

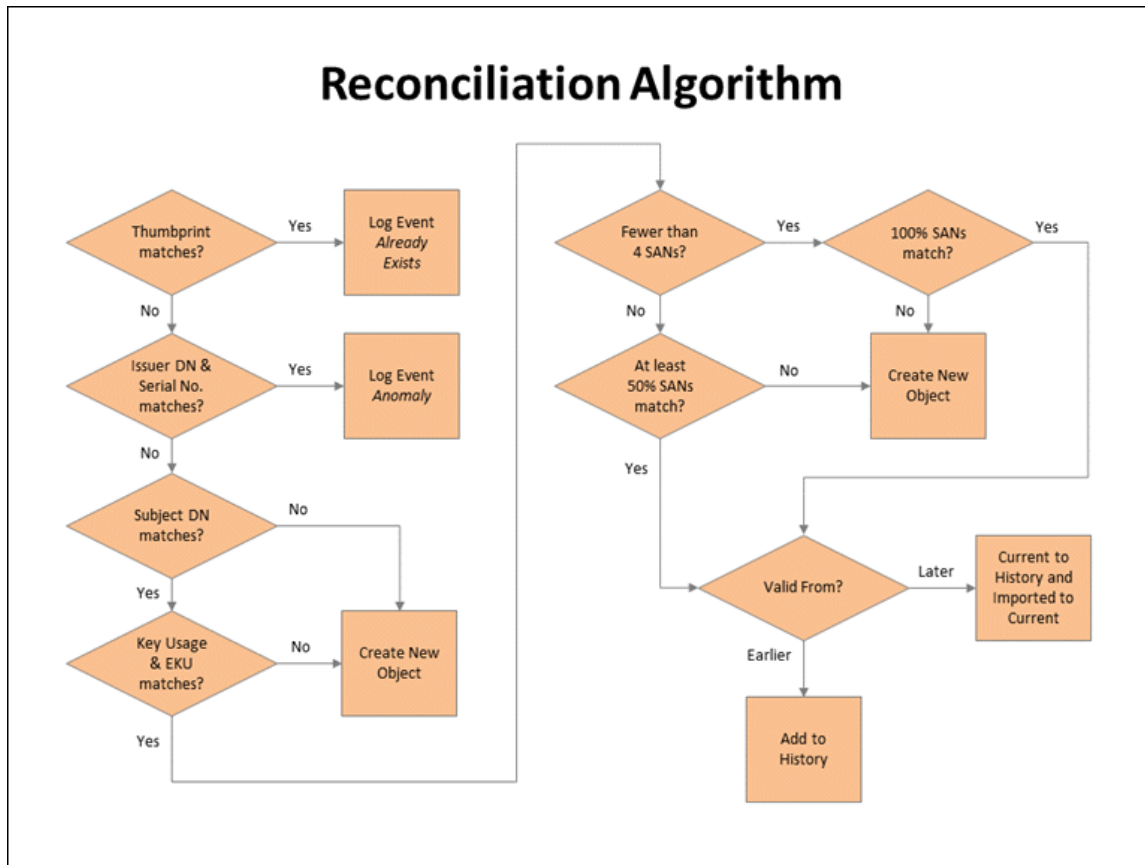
Below the table is a 'Placement Preview' section. It shows a table with the following data:

Placement Rule	New Certificates	New Locations
78 certificates and 88 devices that do not match any rule - Policy \Resources		

At the bottom of the 'Placement Preview' section is a checkbox labeled 'Exclude preview and place certificates automatically next time this job runs' and a 'Place Now' button.

CA Import reconciliation rules

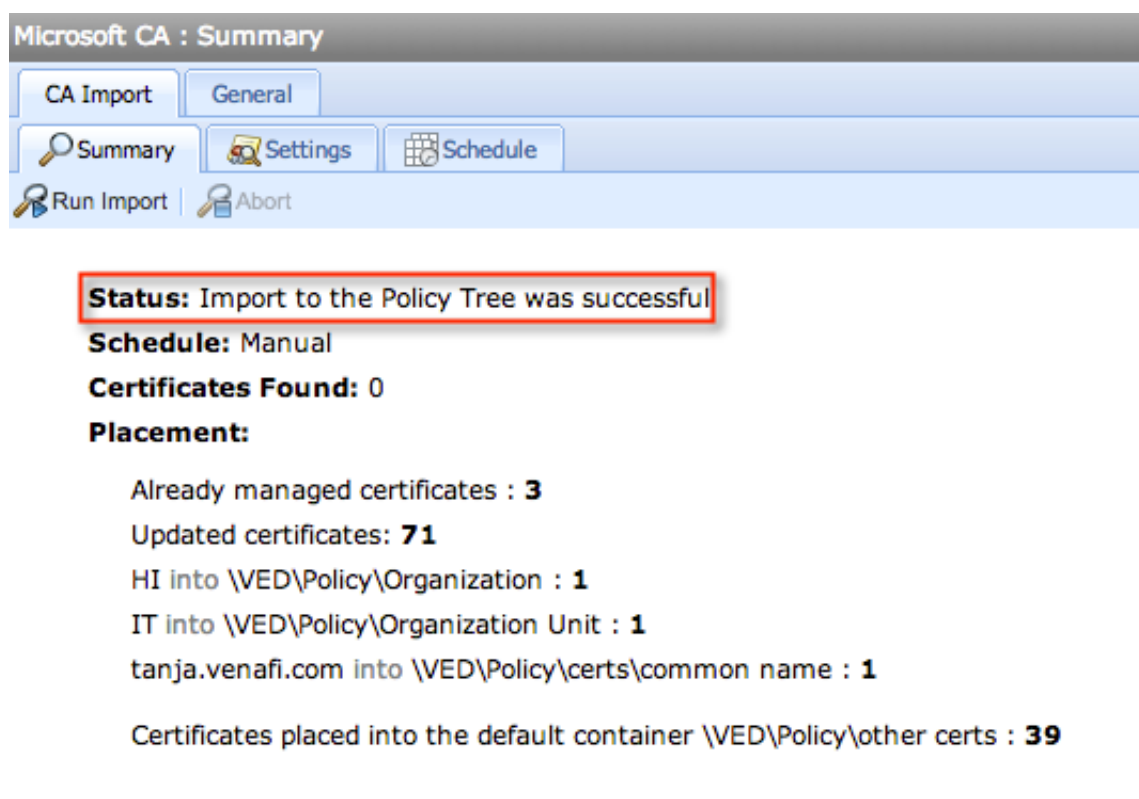
The following flowchart displays Trust Protection Platform's rules for reconciling certificates. During a CA import, these rules are used to determine how a certificate is treated and classified.



Verify certificate import results

When certificates have been placed, Trust Protection Platform displays the message, *Import to the Policy Tree was successful.*

You'll also see a summary of the placement totals based on reconciliation and placement rules. For more information, see ["CA Import reconciliation rules"](#) above.



The categories under Placement are:

Category	Description
Already managed certificates	This exact certificate (ex: including serial number and thumbprint) is already known to Trust Protection Platform. Nothing is done because this Discovery gave us no new information. The information is discarded.
Updated Certificates	When the certificate was imported, Trust Protection Platform found something in the policy tree that had a different version (newer or older) of the same certificate and instead of following the placement rules that would normally have applied, Trust Protection Platform updated the certificate object and added the certificate to be either the current certificate or historical/previous version depending on the "Valid from" information.

Category	Description
<code><name></code> into <code><folder></code>	Shows a summary of how many certificate objects are created for each placement rule.
Certificate default container <code><folder></code>	The certificate objects created from the discovery that are new (they didn't match any existing placed into certificates), and they didn't match any placement rules. These certificate objects were placed in the default folder, which is shown.

In the Policy tree, the certificates are placed in folders according to your placement rules. Each type of certificate has its own icon. For more information, see ["Overview of certificate types" on page 139](#).

Icon	Description
	Server Certificates
	User Certificates
	Client Device Certificates

Things you can do to correct errors:

- ["Changing a certificate's type" on page 35](#)
- Creating, modifying, and deleting placement rules for CA import

Enable or disable a CA import service module

Typically, enabling and disabling various Trust Protection Platform service modules on each instance of Trust Protection Platform server is a way of managing resource allocations. For example, you might enable certificate importing on one instance and disable it on all other instances.

After you disable the CA import service module, you won't have the ability to import certificates using that instance of Trust Protection Platform until you enable it again using either Venafi Configuration Console (VCC) or Policy Tree.

TIP In Trust Protection Platform 19.1, *CA Import* is called *Certificate Import* in the Aperture user interface. This is a required but temporary discrepancy as CA import functionality is migrated from Policy Tree to Aperture.

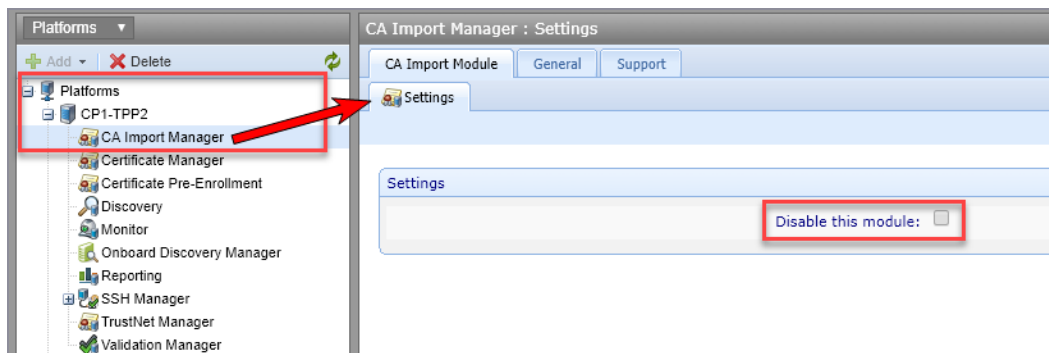
To enable or disable the CA import module using VCC

1. On the application server where you're running Trust Protection Platform, open **Venafi Configuration Console**.
2. In the left panel, click the **Product** node.
3. In the center panel under TLS Protect, click **CA Import**, then in the action panel on the right click **Enable** or **Disable**.

For more information about VCC, see [Venafi Configuration Console](#).

To enable or disable the CA import module using Policy Tree

1. From the [Platform menu bar](#), click Policy Tree.
2. In the **Platforms** tree, find and click the server that holds the CA import module you want to disable.
3. Click the **CA Import Manager** node.
4. On the **Settings** tab, select **Disable this module** if you want to disable it on the current instance of Trust Protection Platform.



5. Click **Save**.

4

Managing network certificates and private keys

Besides managing your certificate lifecycle, Venafi Trust Protection Platform provides extensive certificate and private key management features.

To acquire existing certificate and private key files, you can manually import certificate and private key files to Trust Protection Platform or you can allow Trust Protection Platform to extract certificates and private keys directly from managed applications. Once certificates and private keys are securely stored in the Trust Protection Platform database, you can install, or “push,” a certificate and private key to other servers in your network—or, if preferred, you can simply download the certificate and private key, then manually install them yourself.

Venafi Trust Protection Platform™ simplifies the process of managing digital certificates through their lifecycles. When a certificate is brought under management, Trust Protection Platform monitors the certificate and provides current information on the certificate status. When a certificate nears the end of its lifecycle, Trust Protection Platform provides notifications so you can renew and install the certificate before it expires.

If the certificate is configured for enrollment, Trust Protection Platform interfaces directly with CA to initiate certificate renewal and key generation requests according to organization-defined workflow and approved folders. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the Secret Store. The administrator can then download the certificate from the Secret Store and install it on the target system(s).

If the certificate is configured for Provisioning, Trust Protection Platform automatically requests, renews, and installs the certificate on its associated application(s), ensuring that the certificate is reliably deployed and managed.

Besides managing your certificate lifecycle, Trust Protection Platform also provides extensive certificate and private key management features. To acquire existing certificate and private key files, you can manually import certificate and private key files to the Trust Protection Platform database or you can allow Trust Protection Platform to extract certificates and private keys directly from managed applications. Once certificates and private keys are securely stored in the Trust Protection Platform database, you can install, or “push,” a certificate and private key to other servers in your network—or, if preferred, you can simply download the certificate and private key, then manually install them yourself.

This chapter contains the following topics:

Bringing network certificates under management	135
Managing certificate configuration	139
Associating certificates with applications	202
Renewing a certificate manually	214
About clearing certificate workflow errors	218
About revoking certificates manually	220
About Revocation Checking	226
Validating Certificate Revocation Lists - Overview	236
Pushing Certificates and Private Keys to Applications	249
ACME integration with TLS Protect	251

Bringing network certificates under management

After you run a discovery job, you can place the discovered network certificates under management. This is the fastest and easiest way to bring network SSL certificates under management because the Discovery feature automatically populates many certificate settings.

About importing existing certificates

You may want to bring a certificate that wasn't issued by Trust Protection Platform on board. You can create a placeholder certificate in TLS Protect and then import the existing certificate from your server so that you have a current instance of it.

The advantages of importing a certificate include the following:

- Ability to monitor it for expiration
- Validation that it is meeting policy and audit requirements
- Use of daily validation to ensure the certificate is installed in the correct location
- Making renewal of the certificate easier when the expiration date is near

For more information in importing certificates, see ["Importing an existing certificate" below](#).

Importing an existing certificate

You may want to bring a certificate that wasn't issued by Trust Protection Platform on board. You create a certificate placeholder and set the Management Type to Monitoring. After the certificate is created in inventory, use the Upload option to upload the certificate file into the placeholder you created in Inventory.

To create a certificate placeholder

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. On the Certificates page, click **Create a New Certificate**.
3. Select the appropriate **Certificate Folder**.
4. Click **Submit**.

5. Fill in the details as needed.

IMPORTANT Be sure to select **Monitoring** as the Management Type.

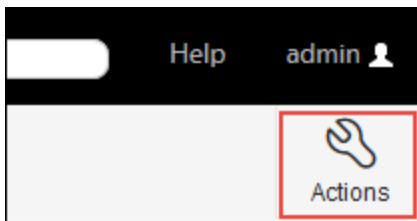
6. When you're done, click **Submit**.

To import a certificate

NOTE You must have *View* and *Write* permissions to the certificate. If the certificate is in a format that includes the private key, you must also have the *Private Key Write* permission to the certificate.

Supported keystore upload types are: PEM, DER, PKCS#7, and PKCS#12.

1. From the [TLS Protect menu bar](#), click **Inventory**> **Certificates**.
2. Locate the certificate you created as a placeholder, and then click its name.
3. Click **Actions**.



4. Click **Import**.
5. In the Import Certificate window, do one of the following:
 - Drop the new certificate file into the box.
 - Click inside the box to upload the certificate.
 - Paste the certificate text into the box.
 - Click the **Find the certificate in a network location** link to enter a URL and port from which to retrieve an existing certificate.
6. (Conditional) If required, enter the private key password.
7. Click **Submit**.

In the Import Certificate window you can preview the new values, as populated by the certificate you just imported.

8. Click **Import**.
9. In the certificate's details page, click **Show All Properties** to see the updated values of the certificate.

NOTE When you upload a certificate, the renewal values will automatically update to match the certificate that was just uploaded.

Retrieving certificates

The  Retrieve Certificate option retrieves a certificate from a designated host or IP address and port.

If the current certificate is managed at the *monitoring* level, you can use this option to update the certificate in the Trust Protection Platform database after you have manually renewed the certificate on the target device so that Trust Protection Platform can validate the certificate.

If the current certificate is managed at the *enrollment* or *provisioning* levels, you can use this option to retrieve the certificate from the CA. Under Enrollment, the administrator could then download the certificate and manually install it on the associated servers. Under Provisioning, Trust Protection Platform would then automatically install the certificate on the certificate object's associated applications.

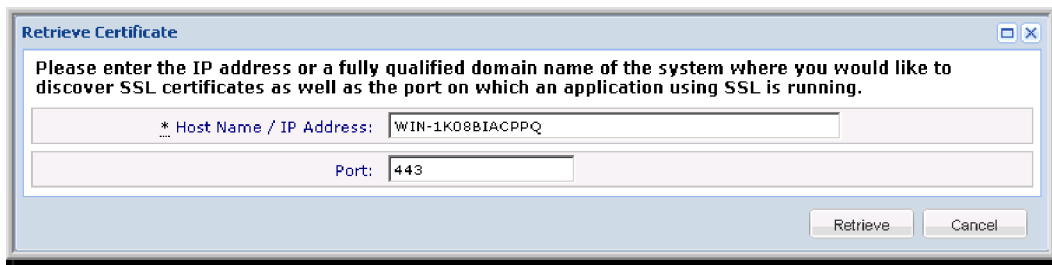
NOTE Before completing this task, keep the following in mind:

- In order to retrieve a certificate, you must have View and Write permissions to the associated certificate object.
- This option is available only in Policy Tree.
- You can set up a notification to alert you when the certificate has been updated on the target application. For more information, see ["Review validation results" on page 548](#).

To retrieve a certificate

1. From the [Platform menu bar](#), click Policy Tree.
2. In the **Policy** tree, select the certificate object associated with the certificate file you want to import.
3. Click the **Certificate > Settings** tab.

4. Click  **Retrieve Certificate**.



5. Enter the hostname or IP address and port of the server from which you want to retrieve the certificate.

Trust Protection Platform automatically populates the Certificate object with the certificate data.

6. When finished, click **Apply/Save**.

Re-import a certificate from a network address

When you have a certificate being tracked in Trust Protection Platform, you may find that you want to import an updated version of the certificate from a network source. For example, if the certificate is renewed outside of Trust Protection Platform, you need to get the new certificate into the system easily.

You can import a certificate directly from a URL using the following procedure.

Import a certificate from a network address

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. Locate the certificate you want to update.
3. From the quick action button, click **Import**.
4. Click **find the certificate in a network location**.
5. Enter the hostname or IP address where the certificate is installed.
6. Enter the port number that the certificate is installed on.
7. Click **Find**.
8. Review the new certificate values, then click **Import**.

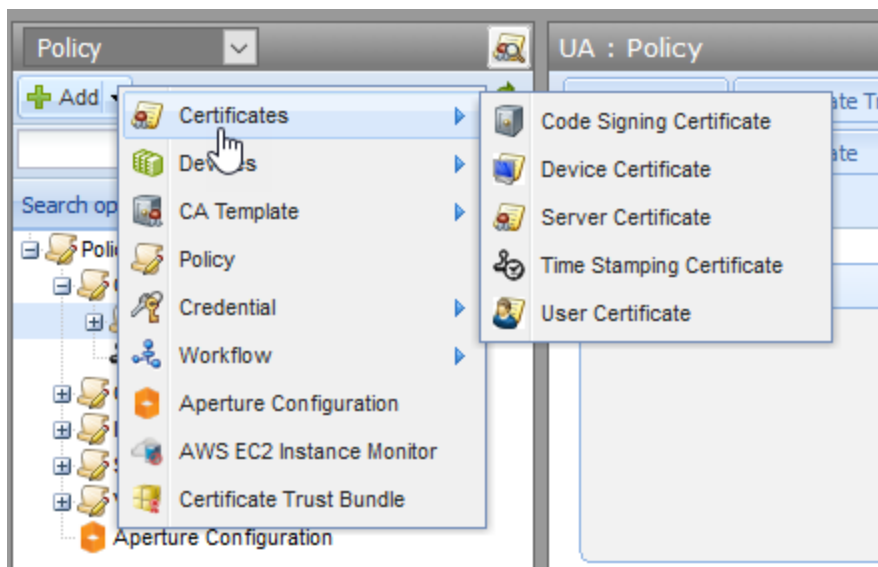
Managing certificate configuration

This section provides the information you need to effectively manage certificate objects for network certificates.

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:

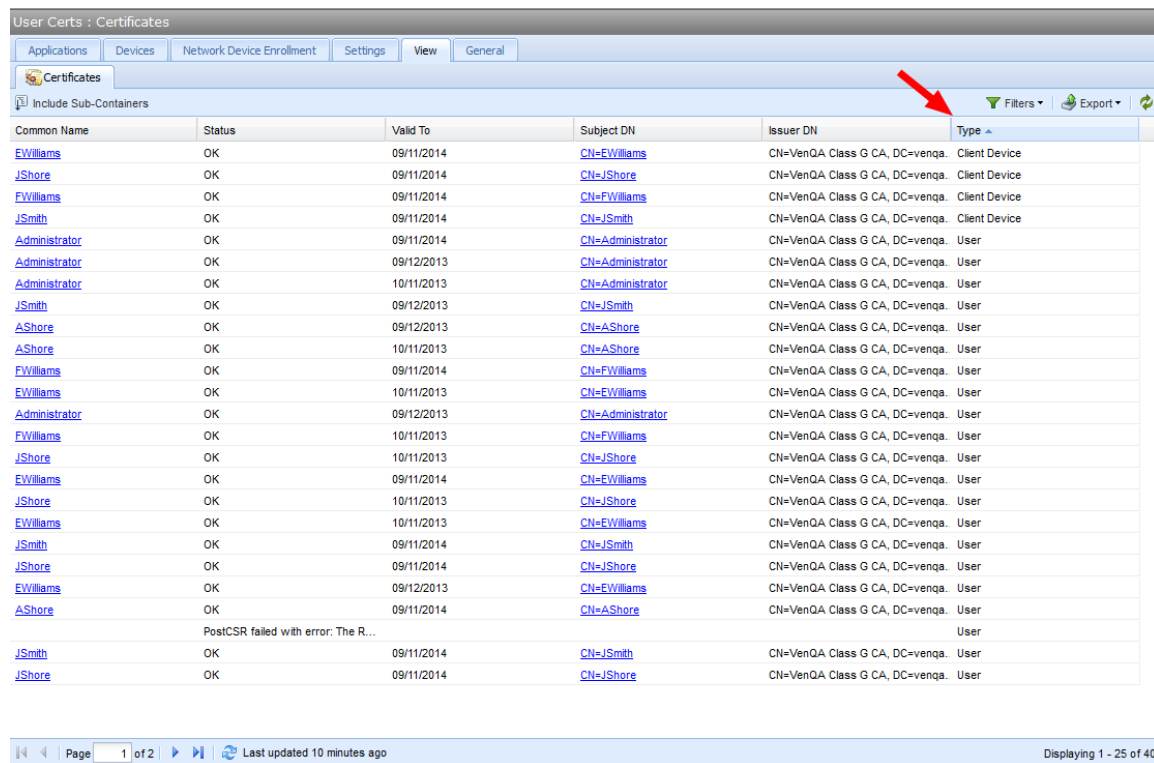
Certificates / AShore-Client						
AShore-Client						
Client Device Certificate						
Issuer	Common Name	Organization	Organizational Unit	Locality	State / Province	Key Size
Self Signed	ashore@venqa.venafi.com	Venafi Inc.	Development	Salt Lake City	Utah	1024
Key Usage		Enhanced Key Usage				
Digital Signature, Key Encipherment (a0)		Client Authentication (1.3.6.1.5.5.7.3.2)				

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.



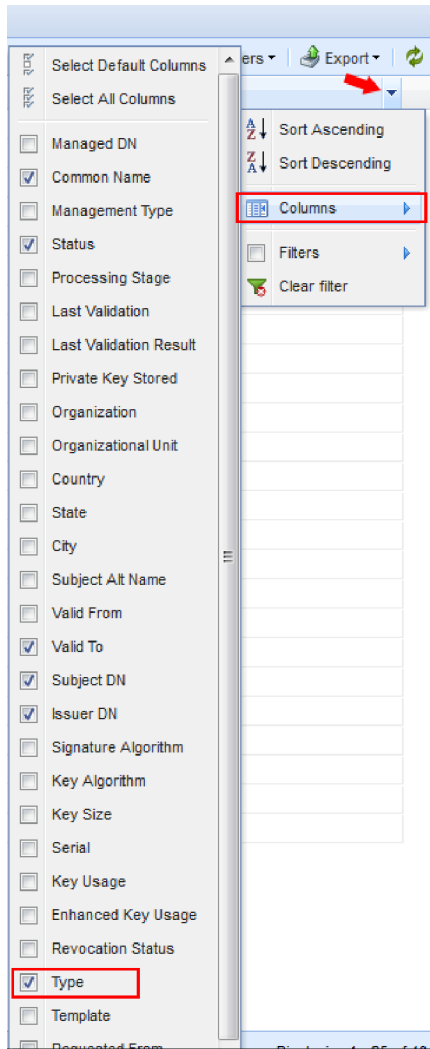
The screenshot shows the 'User Certs : Certificates' interface. The 'View' tab is selected. A red arrow points to the 'Type' column header in the certificate grid. The grid lists various certificates with columns for Common Name, Status, Valid To, Subject DN, Issuer DN, and Type.

Common Name	Status	Valid To	Subject DN	Issuer DN	Type
EWilliams	OK	09/11/2014	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	Client Device
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	Client Device
FWilliams	OK	09/11/2014	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	Client Device
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	Client Device
Administrator	OK	09/11/2014	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	09/12/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	10/11/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
JSmith	OK	09/12/2013	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	09/12/2013	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	10/11/2013	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
FWilliams	OK	09/11/2014	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	10/11/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
Administrator	OK	09/12/2013	CN=Administrator	CN=VenQA Class G CA, DC=venqa.	User
FWilliams	OK	10/11/2013	CN=FWilliams	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	10/11/2013	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	09/11/2014	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	10/11/2013	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	10/11/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User
EWilliams	OK	09/12/2013	CN=EWilliams	CN=VenQA Class G CA, DC=venqa.	User
AShore	OK	09/11/2014	CN=AShore	CN=VenQA Class G CA, DC=venqa.	User
	PostCSR failed with error: The R...				User
JSmith	OK	09/11/2014	CN=JSmith	CN=VenQA Class G CA, DC=venqa.	User
JShore	OK	09/11/2014	CN=JShore	CN=VenQA Class G CA, DC=venqa.	User

Page 1 of 2 | Last updated 10 minutes ago | Displaying 1 - 25 of 40

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**.



Configuring the certificate management level

To address the needs of diverse organizations with varied security requirements, Trust Protection Platform provides four levels of certificate management:

Monitoring	At this level, organizations can continuously monitor key and certificate assets for improved inventory and risk mitigation. Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform sends dynamically-generated expiration and escalation messages to certificate owners, consumers, and approvers. At the monitoring level of certificate management, however, Trust Protection Platform does not renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then retrieve and install the renewed certificate. Once the certificate is manually installed, Trust Protection Platform can validate the certificate is installed and properly configured. Monitoring is enabled in the Certificate object configuration.
Enrollment	At this level, Trust Protection Platform interfaces directly with Certificate Authorities (CAs) to initiate and auto-enroll new or to-be-renewed certificate and key generation requests according to organization-defined workflow and approved folders. Trust Protection Platform automatically generates and submits CSRs to CAs using the parameters defined in designated CA Template objects. If preferred, administrators can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the Secret Store. The administrator can then download the certificate from the Secret Store and install it on the target system(s). Enrollment is enabled in the Certificate object configuration.

For an explanation of the managed stages of the certificate lifecycle, see ["About certificate lifecycle management" on page 27](#).

Provisioning At this level, Trust Protection Platform provides fully automated lifecycle management—it automatically requests, installs, renews, and monitors your system certificates and keys on a comprehensive set of systems and applications, producing consistent and repeatable processes that improve security, and operational and compliance risk postures.

Provisioning is enabled in the Certificate object configuration.

For an explanation of the managed stages of the certificate lifecycle, see ["About certificate lifecycle management" on page 27](#).

Unassigned Unlicensed Trust Protection Platform certificates that do not allow network validation, expiration monitoring, enrollment, provisioning, or onboard validation. However, they are included in selected reports and on the dashboard.

To change a certificate's management type, see ["Changing the management type to Provisioning" on page 511](#)

Configuring certificate objects

You can change certificate settings in the Policy tree.

IMPORTANT You must have the *Write* permission to a certificate object before you can configure it.

To configure a certificate object

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. In the Policy tree, select the certificate object you want to configure.

3. Click the **Certificate > Settings** tab.
4. Complete certificate settings, and then click **Apply/Save**.

For more information, see ["About local certificate settings" on page 303](#) in the Venafi Trust Protection Platform *Trust Protection Platform Certificate Management Guide*.

About certificate object settings

The *certificate object* provides the information Trust Protection Platform needs to monitor, enroll, and provision network certificates.

Additionally, consider managing certificate object settings via policy. For more information, see [Using policies to manage encryption assets](#) in the *Venafi Trust Protection Platform Administration Guide*.

The following table describes the configuration settings for a network certificate object. The second column indicates if the setting may also be managed via Policy.

Field	Policy	Description
 Refresh	n/a	Refreshes the contents of the current page.
 Print	n/a	Prints the contents of the current Detail View.

Certificate Tab

Summary Tab

Provides a snapshot of the current certificate. It lists the certificate status, all associated applications, the certificate signature chain, and the certificate details.

Any user with the *write* permission to the certificate can access all of the options in the Certificate Summary tab and view all summary data, including information about the certificate's associated applications regardless of whether the user has permissions to the associated applications themselves.

For more information, see ["About a certificate's summary \(Policy Tree\)" on page 311](#).

Field	Policy	Description
 Restart	n/a	Clears all errors and stages on the certificate and its associated application(s), then restarts processing from the beginning. In Policy Tree, this option is available under  Fix > Restart Processing from the Beginning. This option is provided for circumstances in which the certificate or application was misconfigured. This option allows you to restart the certificate processing so the correct information can be used. For example, if you misspelled the certificate's common name, you could correct the spelling error, then restart the renewal process so the change is reflected in the new certificate. You can use the <i>Restart</i> option at any point during the renewal process. This option is relevant only to certificates managed under Enrollment or Provisioning. For more information, see "About clearing certificate workflow errors" on page 218.
 Retry	n/a	Clears the certificate error, then retries the last processing stage. In Policy Tree, this option is available under  Fix > Retry Last Failed Operation. If the certificate is currently in an error state, this option clears the error, then queues the certificate to retry the current stage. For example, if a certificate was configured with an invalid CA template, you could reconfigure the CA template, and then click <i>Retry</i> to resume the renewal process. If there is an error on the certificate's associated application(s), then Trust Protection Platform reattempts to install the certificate on the associated application(s). Disabled applications are skipped. This option is available only for certificates managed under Enrollment or Provisioning.

Field	Policy	Description
For more information, see "About clearing certificate workflow errors" on page 218.		
 Reset	n/a	Clears errors and stages on the certificate and its associated applications, then stops processing. In Policy Tree, this option is available under  Fix > Reset Errors and Stop Operation. This option is provided for circumstances in which there is an error at some stage of the certificate lifecycle and you decide to abort the current renewal process. For example, if a certificate completed the enrollment process, but failed when installing on one of the associated applications, you could manually install the certificate on the application, and then click Reset to clear the error. In this instance, no further processing would be necessary. This option is relevant only to certificates managed under Enrollment or Provisioning. For more information, see "About clearing certificate workflow errors" on page 218.
 Validate Now	n/a	Instantly runs a validation check on the current certificate according to the settings configured in the object's Validation tab. For more information on Certificate object validation, see About certificate and application validation.
 Revoke/Revoke and Disable	n/a	The Revoke option submits a revocation request to the certificate CA. The Revoke and Disable option sends a revocation request to the certificate CA and disables the current Certificate object. If you disable the Certificate object, Trust Protection Platform stops all certificate processing—that is, it will not monitor, enroll, or provision the certificate.

Field	Policy	Description
		For more information, see "About revoking certificates manually" on page 220.
Change Certificate Type	n/a	Allows you to change the certificate type of a certificate in case it is misclassified. To see a list of certificate types, see "Overview of certificate types" on page 139.
Certificate Status		
Status	n/a	Just below the Certificate Status title bar, Trust Protection Platform displays the current status of the certificate object, including the following common messages:  There is no processing and the certificate is working.  The certificate is being processed. The status field provides a description of what is happening.  There is a problem and the certificate is not functioning. The status field provides a description of the problem.  Workflow request has been rejected.
Processing Stage	n/a	If the certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle. For example, if Trust Protection Platform is currently waiting to retrieve the certificate from the CA, it displays the following: <pre>700 (Retrieving certificate from CA)</pre> If the certificate is not currently under processing, the processing stage is "None." If processing is disabled on the application, the processing stage is "n/a" (not applicable).

Field	Policy	Description
The processing stages listed are specific to each device. For more information, see "About certificate lifecycle management" on page 27.		
Certificate Processing	n/a	Indicates if the certificate processing is enabled or disabled. If the Certificate object is disabled, Trust Protection Platform does not monitor, validate, enroll, or provision the certificate. Certificate Processing is enabled or disabled on the Settings tab.
Expiration Date	n/a	The date the certificate expires.
Last Validation	n/a	Time and date of the last validation.
Network Result	n/a	Result of the most recent Network Validation.
Associated Applications	n/a	All applications where the current certificate is installed.

Settings Tab



Renew Now n/a

Queues the certificate for renewal. Error and status attributes are cleared on the certificate and its associated application(s).

NOTE This option is available only for certificates managed under Enrollment or Provisioning.

In order for Trust Protection Platform to automatically renew a certificate, the **Processing Disabled** option must *not* be selected.

In Policy Tree, the **Renew Now** option is available in the Certificate Summary page. In Policy Tree, the **Renew Now** option is available in the **Certificate Settings** page.

Trust Protection Platform only attempts the renewal; it does not revoke the existing certificate. For information on revoking a certificate, see ["About revoking certificates manually"](#) on page 220.

Field	Policy	Description
		A user must have <i>write</i> permissions to manually restart a certificate renewal. For more information, see "Renewing a certificate manually" on page 529.
 Download	n/a	This option is available only in Policy Tree. Downloads the certificate and, optionally, the private key and root chain from the Trust Protection Platform database and allows you to save it to a Base64, DER, PKCS#7, or PKCS#12 formatted file. If you select PKCS#12 format, you can define a password that will be required to access the downloaded certificate and private key. For more information, see "Downloading certificates, private keys, and root chains" on page 453.
 Import	n/a	This option is available only in Policy Tree. Allows you to copy and paste a Base64-encoded certificate file (and, optionally, the private key) into Policy Tree. Trust Protection Platform automatically populates the certificate object with the certificate data and, when you save the certificate object, it archives the certificate file in the Trust Protection Platform database. If the uploaded certificate includes the private key, you must specify the password required to access the private key. You must have the <i>view</i> and <i>write</i> permissions to the certificate object to import a certificate. If the certificate is in a format that includes the private key, you must also have the <i>Private Key Write</i> permission to the certificate object. For more information, see "Importing an existing certificate" on page 135.
 Retrieve Certificate	n/a	This option is available only in Policy Tree. Retrieves the certificate from a designated host or IP address and port.

Field	Policy	Description
		Trust Protection Platform supports both IPv4 and IPv6 connections.
		If the current certificate is managed at the Monitoring level, you can use this option to update the certificate in the Trust Protection Platform database after you have manually renewed the certificate on the target device.
		You can set up a Notification to alert you when the certificate has been updated on the target application. For more information on this configuration, see "Review validation results" on page 548 .
		If the current certificate is managed at the Enrollment or Provisioning levels, you can use this option to retrieve the certificate from the CA.
		You must have the <i>view</i> and <i>write</i> permissions to the certificate object to retrieve a certificate.
		For more information, see "Retrieving certificates" on page 137 .

General Information

Certificate Name	No	Unique name for the certificate object. This is a mandatory field.
Description	No	Use to describe what the certificate is used for.
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	Policy	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, 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, discontinuous users and groups.
		You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Approver		User or group Identities assigned to approve workflows (certificate approval or injection command) for the current certificate object. For more information on defining workflow objects, see Workflow management.

Default approver = master administrator

To select the Certificate object approvers

- 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

Field	Policy	Description
		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. Press Shift+click to select multiple, contiguous users and groups. Press Ctrl+click to select multiple, discontinuous users and groups. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Processing Disabled	No	Disables monitoring, enrollment, and provisioning of the current certificate. This means that Trust Protection Platform does not generate notifications, validate, or attempt renewal for the current Certificate object. This option is useful when you are building the certificate configuration but it is not yet complete. Select Processing Disabled to disable the object until you're ready for it to be active. In this way, you can avoid system processing errors due to an incomplete configuration.
Management Type		Level where subordinate certificates are to be managed. To learn how to change a certificate's management type, see "Changing the management type to Provisioning" on page 511. Trust Protection Platform provides the following levels of certificate management for Kubernetes Policy, Cluster, and Namespace objects: ▪ Monitoring: Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform notifies the administrator. It does not, however, renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then

Field	Policy	Description
		retrieve and install the renewed certificate.
		▪ Enrollment: Trust Protection Platform can automatically generate and submit CSRs to Certificate Authorities using the parameters defined in designated CA Template objects. If preferred, the administrator can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the central database. The administrator must then download the certificate from Trust Protection Platform and install it on the target systems. ▪ Provisioning: Trust Protection Platform manages the entire certificate lifecycle—it automatically requests, installs, and monitors your system 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.

You can manage this setting at the policy level. To configure the setting via Policy, go to the **Settings > Certificate** tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "[Policy object certificate settings](#)" on page 319.

CSR Generation



Determines how CSRs are generated.

- **Service Generated CSR:** Trust Protection Platform automatically generates the CSR. If a certificate is associated with multiple applications, the CSR will be centrally generated so Trust Protection Platform can push the private key to both applications.

Field	Policy	Description
		Remote CSR generation does not allow private key sharing across multiple applications. Only a 1-1 relationship is supported. ▪ User Provided CSR: CSR is manually generated by the administrator, then uploaded to Trust Protection Platform. DID YOU KNOW? Today, you can specify SANs on your CSR, but <i>only if the CSR has no embedded SANs</i>. Not all CAs support adding additional SANs (<i>additive SANs</i>); so to allow maximum compatibility across many CAs, Trust Protection Platform prevents the use of additive SANs. Trust Protection Platform always generates CSRs in compliance with the certificate object's current parent policy. If the CSR is user-submitted, Trust Protection Platform does not accept the CSR unless it is "in policy." You can manage this setting at the policy level. To configure the setting via policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319 in the <i>Venafi Trust Protection Platform Certificate Management Guide</i>.
Generate Key/CSR on Application		Determines where the CSR and the private key are generated. If you do not select this option, the CSR and the private key are centrally generated on the Trust Protection Platform server, then securely copied to the application. If you do select this option, the CSR and the private key are locally generated on the application's server. In the case of central generation, the certificate and private key are archived in the Trust Protection Platform database. However, for remote generation, only the certificate is stored in the database.

Field	Policy	Description
		You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319. IMPORTANT When one or more of the following items are true, Remote Generation is <i>not</i> supported and, therefore, the <i>Generate Key/CSR on Application</i> setting is ignored. ■ You're using a driver that does not support remote generation. To learn which drivers support remote generation, see Supported integrations: devices, applications, services and features supported by Venafi. ■ You're using a self-signed CA template to enroll a certificate; self-signed CA templates do not work with remote generation. This is because Trust Protection Platform requires that the private key be stored centrally so that it can be used to sign the self-signed certificate. ■ Your certificate is associated with more than one application; to work correctly, the certificate must be associated with <i>one</i> application. ■ You have not set the certificate's management type setting to Provisioning. ■ You're doing one-to-many provisioning.
Hash Algorithm		For the certificate signing request, choose either SHA-256, SHA-384, or SHA-512. The default is SHA-256. See About signing algorithms.

Field	Policy	Description
Upload CSR	No	Allows the administrator to paste the CSR data or upload a CSR file to the Trust Protection Platform database. The CSR file must be Base64 encoded. If Service Generated CSR is selected, then the uploaded CSR values are added only to the unlocked SubjectDN fields that are editable. No check is made to ensure that the values adhere to the policy. If User Provided CSR is selected, then the uploaded CSR values must adhere to the policy before they are applied to the Certificate object. If they do adhere to the policy, they are added to the certificate and stored in the Trust Protection Platform database when the Certificate object is saved. For more information, see "Manually uploading the CSR" on page 216. If the CSR is user provided, you may also want to upload the private key so it is archived in the Trust Protection Platform database. Trust Protection Platform must have a copy of the certificate's private key to provision certificates and key pairs. For more information, see "Manually Uploading the Private Key" on page 218.
Subject DN		
Common Name	No	Typically, the fully qualified domain name.
Subject Alt Name	No	The DNS-based Subject Alt Name(s) (SANs) associated with the current certificate. NOTE Symantec has a limit of 20 SAN entries. If you enter more than 20 SANs, the Symantec CA returns the following error: "The specified Certificate Authority has a limit of 20 SubjectAltNames."

Field	Policy	Description
		Trust Protection Platform includes the SANs in the certificate CSR. If the CA does not accept SAN entries in the CSR (RedHat is the only currently supported CA that does not accept SAN entries in the CSR), then Trust Protection Platform provides the SAN values to the CA out-of-band during the certificate approval process. If the certificate requires manual approval, Venafi TLS Protect does not include the SAN values in the CSR. Instead, it notifies the approver to provide the DNS SAN values when approving the certificate. To enable Venafi TLS Protect to provision SAN certificates, your configuration must meet the following criteria: Verify that your CA supports DNS-based SAN values. NOTE DNS SANs are included in the Unified Communications Certificates that are used with Microsoft Exchange 2007 and Microsoft Office Communications Server. At present, the Entrust Security Manager CA does not support DNS-based SANs. If you use Microsoft, RedHat, or Symantec CAs, you must verify the SAN feature is enabled on your CA engine. If you enter a SAN value but the SAN feature is not enabled on your CA, the CA returns the following error when Venafi TLS Protect attempts to submit the CSR: Stage 400 (Creating CSR) SubjectAltName not supported by Application and CA. The Subject Alt Name Enabled option must be enabled on the certificate's associated CA template object; otherwise, the CA template object will not accept CSRs with SAN values. For more information, see your associated CA template object configuration in Managing certificate authority (CA) templates.

Field	Policy	Description
		If you do not enable the Subject Alt Name Enabled option on the certificate's associated CA template object, Trust Protection Platform returns the following error when it attempts to submit the CSR: Stage 400 (Creating CSR) SubjectAltName not supported by Application and CA. If you enable the Generate Key/CSR on Application option in the current Certificate object, you must verify that the Application driver for the certificate's consumer applications can generate a CSR with SAN values. IMPORTANT At present, only the GSK application can generate a CSR with SAN values. To enable the GSKit 7.x driver to generate a CSR with SAN values, you must set the SAN support value to <i>true</i> in the ikminit.properties file as follows: DEFAULT_SUBJECT_ALTERNATIVE_NAME_SUPPORT=true The ikminit.properties file may be written to several locations. Search for and change all instances of the file in the file system. The default locations are <code>%GSK_HOME%\classes</code> and <code>*c:*</code>. If you enable the Generate Key/CSR on Application option in the certificate object and the certificate's consumer application is an Apache web server or other application that consumes a PEM file in a non-Windows environment, NetScaler device, or an F5 network appliance, then Venafi TLS Protect must provide the SAN values to the CA out-of-band. This is not a problem for Microsoft or RedHat, or Thawte, or Symantec certificates. However, the RSA Keon CA does not accept out-of-band values. If you enable the Generate Key/CSR on Application option in the certificate object and the certificate's consumer application is a GSK keystore, but the SAN feature is not enabled on your CA, then the CA returns the following error:

Field	Policy	Description
Create CSR failed with error: {0}, Subject Alternative Name support not enabled. The error message also provides information about what file needs to be modified to support SAN.		
Organization		Name that uniquely identifies the organization in the certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Organization Unit		Department or division within the organization that is responsible for maintaining the certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
City, State/Province, Country		Location (city, state/province, and country) of your Organization or Organizational Unit. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Domain Whitelist		
Allowed Domains		Enter the suffix of allowed domains. Examples:

Field	Policy	Description
		▪ .com ▪ acme.com ▪ sales.acme.com If you leave this field blank, ALL domains will be allowed.
Allow Wildcards		The default is Yes . Select No to prohibit wildcards.
Allow Duplicate Common and Subject Alternate Names		The default is Yes . Select No to require unique names.
Private Key		
Private Key Stored	No	Indicates whether Trust Protection Platform currently has a copy of the certificate's private key—Yes or No. Trust Protection Platform must have a copy of the private key to provision certificates and key pairs. If Trust Protection Platform does not have a copy of the certificate's private key, then you can do one of the following: Manually import the certificate and private key. For more information, see "Manually Uploading the Private Key" on page 218. If Automate Renewal is selected, you can wait until Trust Protection Platform renews the certificate or click Renew Now  to generate a new key pair.
Algorithm		To see which algorithm types are supported, see Algorithm types supported by Venafi Platform .

Field	Policy	Description
		The Use System Default option means to use whatever algorithm is currently selected as the default for that policy. This setting has its own policy control, which can be set on a per-policy basis. If none are set, it falls back to the global default list configured in VCC. NOTE The most broadly supported elliptic curve is P256. The other curves, P384 and P521, may be rejected by some CAs that support ECC. Venafi supports NIST EC curves, including SECP256. The self-signed CA can generate proof-of-concept self-signed certificates for testing purposes with PQ algorithms and any other algorithm available in the UI. To learn more, see Understanding cryptographic algorithms in Venafi Trust Protection Platform.
Reuse Private Key		Reuses the original private key when renewing the certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Upload Private Key	No	Allows the administrator to paste the private key data or upload a private key file to the Trust Protection Platform database. The private key must be base64 encoded and you must specify the password required to access the private key. You must have the <i>Pprivate key write</i>, <i>view</i>, and <i>write</i> permissions to the Certificate object to upload a private key. If the CSR is user provided, you may also want to upload the private key so it is archived in the Trust Protection Platform database. Trust Protection Platform must have a copy of the certificate's private key to provision certificates and key pairs.

Field	Policy	Description
		For more information, see "Manually Uploading the Private Key" on page 218.
Other Information		You can manage the following settings at the policy level. To configure these settings via Policy, go to the Settings > Certificate tab in the Policy object configuration. The settings defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
CA template		CA template object that Venafi TLS Protect references to generate the CSR and submit it to the CA. To select the CA template object 1. Click the Browse button. The Configuration Object Selector dialog opens. 2. Select a CA template object, and then click Select.
Key Generation		Encryption key used to generate the certificate's private key. Trust Protection Platform uses either an AES-256 software encryption key or hardware keys stored on supported HSM devices to generate certificate private keys. For information on using your own encryption keys, see Managing system credentials in the <i>Venafi Trust Protection Platform Administration Guide</i>.
Disable Automatic Renewal		Disables automatic enrollment and provisioning for the current certificate. This means that Venafi TLS Protect will not attempt to renew or install the current certificate on its own. However, Venafi TLS Protect still provides monitoring, validation, and notification for the certificate object. Trust Protection Platform automatically selects this option when it renews a certificate in response to a SCEP request. For more information, see "Certificate enrollment via SCEP protocol" on page 265.

Field	Policy	Description
Renewal Window		Number of days prior to expiration that Venafi TLS Protect begins the renewal operation. Recommended value = 30 DID YOU KNOW? The default renewal window is 32 days for all newly created DigiCert and Entrust templates.
Validity Period	No	Period of time (in months) that the certificate is valid. The options available in this menu are determined by the Available Validity Periods configured on the CA template object.
Server Type	No	Application where the certificate is installed.
Entrust Certificate Services Settings		When you associate the Entrust Certificate Services template object configuration with the certificate object, you can define additional settings that are specific to the certificate. These settings are passed to the Entrust Certificate Services when Trust Protection Platform renews the certificate. In Policy Tree, you must click the Entrust Certificate Services tab to access the Entrust Certificate Services settings. For more information, see Entrust Certificate Services—certificate settings in the <i>Certificate Authority and Hosting Platform Integration Guide</i>.

Settings

Validity Period	No	Period of time (in months) that the certificate is valid. The options available in this menu are determined by the Available Validity Periods configured in the Entrust Certificate Services template object configuration.
Number of Servers	No	Number of servers the current certificate may be installed on.

Field	Policy	Description
Certificate Owner		Person the Entrust Certificate Services identifies as the certificate owner.
First Name	No	Certificate owner's first name.
Last Name	No	Certificate owner's last name.
Email	No	Certificate owner's email address.
Telephone	No	Certificate owner's telephone number.
RSA Keon Settings		When you associate the RSA CA template object configuration with the Certificate object, you can define additional settings that are specific to the certificate. These settings are passed to the RSA Keon CA when Trust Protection Platform renews the certificate. In Policy Tree, you must go to the RSA tab to access the RSA Keon settings. For more information, see RSA Certificate Manager—certificate settings.
Validity Period	No	Period of time (in months) that the certificate is valid. The options available in this menu are determined by the Available Validity Periods configured in the RSA CA template object configuration. This option is available only if you select Override Default Key Update Policy.
Thawte Settings		When you associate the Thawte CA template object configuration with the Certificate object, you can define additional settings that are specific to the certificate. These settings are passed to the Thawte CA when Trust Protection Platform renews the certificate. In Policy Tree, you must go to the Thawte tab to access the RSA Keon settings. For more information, see .

Field	Policy	Description
Validity Period	No	Period of time (in months) that the certificate is valid. The options available in this menu are determined by the Available Validity Periods configured in the Thawte CA template object configuration. This option is available only if you select Override Default Key Update Policy.
Number of Servers	No	Number of servers where the current certificate may be installed.
Server Type	No	Application where the certificate is installed.
Issuance Settings		These settings define the certificate renewal parameters.
Challenge Credential		Password Credential required to retrieve or revoke a Symantec certificate. The Challenge Credential is given to Symantec when the certificate's CSR is submitted for enrollment. Symantec subsequently requires the Challenge Credential to retrieve or revoke the certificate. To select the Challenge Credential 1. Click the Browse button. The Credential Selector dialog appears. 2. Select the Certificate Credential you created with the Symantec Administrator Certificate, and then click Select. For more information, see Managing system credentials in the <i>Venafi Trust Protection Platform Administration Guide</i>.

Field	Policy	Description
		You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate Authorities tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319 .
Validity Period (Months)	No	Period of time (in months) that the certificate is valid. The options available in this menu are determined by the Available Validity Periods configured in the Symantec CA template object configuration.
License Count	No	Number of licenses (i.e., concurrent installations) to be issued with the certificate.
Server Type	No	Type of server that the certificate is installed on.
Comment	No	Any information you want to store with the certificate.
Symantec Owner		Defines the information for the Symantec Certificate Owner.
First Name	No	Symantec Certificate Owner's first name.
Last Name	No	Symantec Certificate Owner's last name.
Email	No	Symantec Certificate Owner's email address.
Use Certificate Owner	No	Retrieves the Certificate object's Contact Identity information. This option is available only in Policy Tree. If you want to be able to retrieve AD user information for the Symantec Owner settings, you must define the mapping rules for AD User and Group attributes. For more information, see Viewing mapping rules for AD user and group attributes in the <i>Venafi Trust Protection Platform Administration Guide</i>.

Field	Policy	Description
Additional Certificate Fields	No	Your certificate may include additional certificate fields. These are custom fields defined by your organization in the Symantec MPKI Control Center. Venafi TLS Protect includes these values in the certificate signing request it submits to the Symantec CA. If the custom fields are required, you must define the fields in the Certificate object. If you do not complete required custom fields, the Symantec CA will not accept the CSR. If the fields are optional, you can optionally define the fields in the Certificate object.
Associations Tab	No	Lists the applications associated with the current certificate. When you associate an Application object with a certificate and enable processing, Venafi TLS Protect provisions the certificate and private key on the server where the application resides. For more information and details about the options available in the Associations tab, see "Associating certificates with applications" on page 202.
Compliance Tab		The Compliance tab provides an assessment of the certificate's compliance with its parent folder. For more information, see "Determining certificate compliance" on page 330.
Certificate Value	n/a	The Certificate Value column lists the certificate values as they are currently defined in the certificate. Certificate Values are listed as being in  or out  of policy.
Renewal Value	n/a	The Renewal Value column lists the certificate values currently defined in the Certificate object. Renewal values also reflect policy status.

Field	Policy	Description
History Tab	n/a	The Certificate History tab lists the common name, serial number, issuer, and valid dates for each edition of the certificate associated with the current Certificate object. Each time a new certificate is issued or an existing certificate is renewed, Venafi TLS Protect adds another entry to the Certificate object's History tab. The Certificate History tab indicates the certificate(s) for which Trust Protection Platform has submitted a revocation request. For more information, see "About Viewing Certificate History" on page 313.
 Revoke	n/a	Submits a revocation request to the certificate CA for previous versions of the certificate that have not yet expired. For example, if you renew a certificate several months before it expires, you could provision the certificate on all of its associated servers. Then, after ensuring everything is functioning properly, you could revoke all previous, valid versions of the certificate from the Certificate > History tab. For more information, see "About revoking certificates manually" on page 220.
Monitoring Tab		The Monitoring tab defines the parameters for certificate expiration events. The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the channel and notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393. You can define monitoring settings at the policy level. To configure the certificate object's monitoring settings, go to the Settings > Monitoring tab in the Policy object configuration. The certificate object monitoring settings defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object monitoring settings" on page 327.

Field	Policy	Description
Settings		
Disabled		Disables monitoring for the current Certificate object.
Expiration Events		
Start generating events		Number of days before a certificate expires that you want to start generating expiration events.
Send event every		Frequency (in days) at which you want Trust Protection Platform to generate expiration events.
Escalation Expiration Events		
Start escalating events		Number of days before a certificate expires that you want to start generating escalated expiration events.
Send event every		Frequency (in days) at which you want Trust Protection Platform to generate escalated expiration events.
Validation Tab		Trust Protection Platform provides Network Validation for Certificate objects. During the Network Validation process, Trust Protection Platform sends an SSL request to the certificate's server. If the server responds to the SSL request, Trust Protection Platform retrieves the certificate's serial number and compares it to the certificate that Trust Protection Platform has archived for the corresponding Certificate object. The purpose of Network Validation is to confirm that the certificate is functional and to verify that the correct certificate is being used. If the server responds to the SSL request, Trust Protection Platform knows the certificate is functional. When it retrieves the certificate serial number, Trust Protection Platform can determine if the correct certificate is being used. When you enable Network Validation on the Certificate object, the Validation Manager module runs daily validation checks and reports the results on the object Summary and Validation tab.

Field	Policy	Description
For more information, see About certificate and application validation .		
Options		
Disable	No	Disables all validation for the current Certificate object, including all validation-based notifications.
Network Settings		The purpose of Network Validation is to confirm that the certificate is functional and to verify that the correct certificate is being used. Network Validation requires network access to the server where the application is installed.
Validation Disabled		Disables Network Validation for the current Application object, including all related notifications. You can also disable Network Validation at the policy level. To disable Network Validation via Policy, go to the Settings > Certificate tab in the Policy object configuration. Disabling Network Validation in the Policy object disables Network Validation for all subordinate Network Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Validation Host	No	Determines how Trust Protection Platform identifies the host server where the certificate is installed. Use Certificate Common Name: (Default) Uses a DNS lookup to resolve the certificate's Common Name. It then validates the certificate at every IP address returned from the DNS lookup. Venafi TLS Protect can validate using both IPv4 and IPv6 connections. Specify Address: Allows you to specify a single IP address.
Hostname	No	IP address or hostname you want to validate. Venafi TLS Protect supports both IPv4 and IPv6 connections. This option is read only if you select Specify Address.

Field	Policy	Description
Port		Port that the Validation Manager uses to connect to the server where the application is installed. The Validation Manager uses an SSL connection to validate the application's associated certificate. The default port is 443. You can also set the validation port at the policy level. To set the validation port via Policy, go to the Settings > Certificate tab in the Policy object configuration. The validation port defined in the Policy object may be inherited by all subordinate Network Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Status		The following fields display the results of the last validation. These fields are informational only and cannot be edited. For more information on validation status messages, see "Review validation results" on page 548.
Last Validation	n/a	Time and date of the last validation.
Network Result	n/a	Result of the most recent Network Validation.

Field	Policy	Description
General Tab		
Log Tab	n/a	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 tab	n/a	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.

About Subject Alternative Names (SANs)

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. Values can include:

- **DNS names.** This SAN type is the successor to the common name for server certificates. They provide the set of DNS resolvable host names that are valid server endpoints for the certificate. TLS requires that one of the DNS SANs match the host portion of the URL in order to be trusted.
- **Email address.** This SAN type is applicable to user certificates that are used for signing and encrypting emails. The format of email SAN values follows RFC822 (standard Internet email address format) hence the reason this type of SAN is sometimes referred to as an RFC822 SAN.
- **URI.** This SAN type allows to you embed a URL like `https://example.com` into a certificate.
- **IP address.** This SAN type is an alternative to DNS SANs for server certificates. Rather than a DNS resolvable host name, an IPv4 or IPv6 address specified can be used in the URL and as long as there is a corresponding IP SAN in the certificate it would be trusted for a TLS connection.

- **User principal name (UPN).** This SAN type is applicable to user and device certificates that are used for TLS client authentication. The UPN SAN provides the identity (user principal name) of the client to the server. The format of UPN SANs is the same as for email SANs (user@domain) and often UPNs for users are the same as their email address but there isn't a requirement for them to be the same.

UPN SANs are different from the first four SAN types in this list in that they're not defined by RFC5280. They're a special type of SAN that makes use of the "OtherName" SAN type which identifies it as a UPN SAN by a unique OID 1.3.6.1.4.1.311.20.2.3.

Smartcards are a case of TLS client authentication certificates which make use of UPN SANs.

- **Custom OtherName.** A flexible Subject Alternative Name (SAN) option that allows you to specify a custom Object Identifier (OID) and a friendly name.

To use this SAN type, an administrator must first configure the custom OID within the root policy folder of the Policy Tree. This is done by selecting the **Policy** folder, navigating to the **Certificate** tab, and accessing the **Subject Alt Name Definitions** section.

Like the User Principal Name (UPN) SAN, the Custom OtherName SAN enables the configuration of OtherName types on individual certificates, allowing them to be recognized as a Subject Alt Name during certificate issuance

- **Other objects.** A registered Object identifier followed by a value.

Detail in about SANS in certificates can be found in [RFC 5280 section 4.2.1.6](#)¹.

Supported Subject Alt Names in a Certificate object

Most Subject Alternative Names (SANs) are supported in certificate objects.

The following SANs are supported:

- DNS
- Email address
- URI
- IP address

¹The RFC can be found at the following URL: <https://tools.ietf.org/html/rfc5280#section-4.2.1.6>

- Custom OtherName
- User Principal Name (UPN) using OtherName

Controlling SANs via policy in Aperture

Using a policy setting in Aperture, you can control what SANS are allowed for certificate enrollment.

For more on how to control SANS using policy settings in Aperture, see ["Setting policy on a folder" on the facing page](#).

Add a SAN to a Certificate object

1. In the **Policy** tree, open the certificate work object.
2. To add Subject Alt Names, click **Add/Remove**.
3. Select the SAN Type from the drop-down list.
4. Enter the SAN value.
5. Click **Add**.

Troubleshooting adding and removing SANs

In which situations can you add or remove SANs from a certificate or certificate work object?

What is a Service Generated CSR¹?

What is a Manual CSR²?

¹Trust Protection Platform creates a CSR automatically during the enrollment and renewal process. The CSR is generated with the setting you enter on the certificate object.

²Trust Protection Platform uses the CSR you provide during enrollment and renewal. Certificate object settings cannot be changed if a manual CSR is used.

How the CSR is generated	Ability to add or remove
Select Service Generated CSR	SANs can be added and removed at any time. Fully manual way to create a certificate. Fill in the fields manually then issue the certificate when desired.
Select Manual CSR , upload a CSR which contains no SANs	All SANs types can be added or removed at any time. However, DNS out-of-band SANs ¹ is supported by only these CA drivers: Symantec and Symantec LHK. They are the only drivers that can issue certificates with out-of-band DNS SANs.
Select Manual CSR , upload a CSR which contains SANs	SANs cannot be added or removed.
Select Service Generated CSR , upload a certificate which contains no SANs	SANs can be added or removed at any time. Importing the certificate enables Trust Protection Platform's monitoring system. Importing the CSR does not enable monitoring.
Select Service Generated CSR , upload a certificate which contains SANs	SANs can be added or removed at any time. You can also configure all of the other settings on the object.

Setting policy on a folder

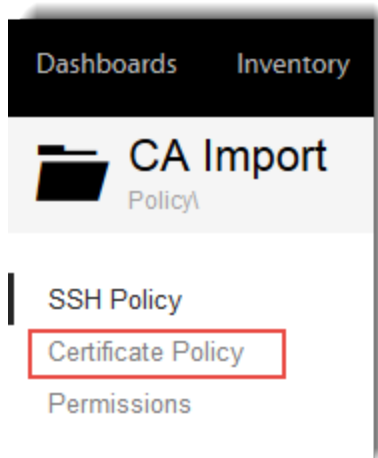
You can configure policy settings for all certificates in the same folder. The configuration is done on the folder.

¹Any Subject Alt Name (SAN) that is added to a certificate object after uploading a CSR that contains no SANs. These SANs are transmitted to the issuing CA along with the CSR, then added to the certificate by the CA.

IMPORTANT You must have the *View* and *Manage Policy* permissions in order to see the **Folders** menu item.

To configure certificate policy on a folder

1. From the **TLS Protect** menu bar, click **Configuration > Folders**.
2. In the list of folders, click the folder that you want to configure.
3. In the sidebar, click **Certificate Policy**.



Field	Description
General Settings	
Contact	User or group Identities assigned to this object. Default system notifications are sent to the contact identities. Default contact = master administrator
Approver	User or group Identities assigned to approve workflows (certificate approval or injection command) for the current Certificate object. For more information on defining Workflow objects, see " Workflow object settings " on page 565. Default approver = master administrator
Management Type	Select either Unassigned, Monitoring, Enrollment, or Provisioning. If you can't make a change, it's because the policy is locked at a higher level.

Field	Description
	Certificate Management types include the following: ◦ Monitoring: Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform notifies the administrator. It does not, however, renew the certificate. The administrator must manually create the CSR, send it to the Certificate Authority (CA), then retrieve and install the renewed certificate. ◦ Enrollment: Trust Protection Platform can automatically generate and submit CSRs to Certificate Authorities using the parameters defined in designated CA Template objects. If preferred, the administrator can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the central database. The administrator must then download the certificate from Trust Protection Platform and install it on the target systems. ◦ Provisioning: Trust Protection Platform manages the entire certificate lifecycle—it automatically requests, installs, and monitors your system 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.
Subject DN	
Organizational Unit	Department or division within the organization that is responsible for maintaining the certificate.
Organization	Name that uniquely identifies the organization in the certificate.

Field	Description
City / Locality	The city or locality of the organization in the certificate.
State / Province	The state or province of the organization in the certificate.
Country	The country of the organization in the certificate.
Allow Domain Component	Check to allow domain component usage for certificates in this folder. This could allow you, for example, to use client authentication certificates to restrict access of the certificate to the sub-domain specified on the certificate using the domain component attribute. This setting should only be used if the application server you are authenticating to is configured to support verification of domain components. You can configure a schedule to run these rules on a regular basis. NOTE This is not a commonly used feature. For more information about domain components, see "About Domain Components" on page 491.
Enrollment Settings	
Renew automatically	Sets an auto-renewal of certificates in this folder based on the specified number of days before expiration.
CA Template	CA Template object that Venafi TLS Protect references to generate the CSR and submit it to the CA.
Key Algorithm	The algorithm to be used for keys assigned to this folder.
Key size (bits)	Certificate's key strength.

Field	Description
	If the key strength value conflicts with what the application can handle/requires, the application ignores the policy and sets the value accordingly. For example, if you set this value to 2048-bit encryption, but the target application cannot handle 2048-bit certificates, Trust Protection Platform generates the certificate CSR using 1024-bit encryption.
Reuse Private Key (Service Generated CSR)	Reuses the original private key when renewing the certificate.
Allows Users to Import Duplicate Certificates and Reuse Private Keys	Controls the reuse of certificates and private keys. When enabled, this permits you to import a certificate even if another certificate with the same private key already exists in the system. It would also allow you to renew a certificate without uploading / re-generating a new private key. When disabled, if you are renewing a certificate with a user-provided CSR, you cannot reuse a CSR that is tied to a private key that has ever been uploaded to Trust Protection Platform. Also, when importing a certificate manually, through WebSDK and Web UI, you won't be able to upload a certificate that is already in the inventory. We recommend you leave this option disabled (unchecked).
CSR Provided By	Determines how CSRs (Certificate Signing Request) are generated. ◦ Service Generated CSR: Trust Protection Platform automatically generates the CSR. ◦ User Provided CSR: CSR is manually generated by the administrator, then uploaded to Trust Protection Platform. Trust Protection Platform always generates CSRs in compliance with the Certificate object's current parent policy. If the CSR is user submitted, Trust Protection Platform does not accept the CSR unless it is "in policy."

Validation Settings

Field	Description
Validate SSL/TLS connections for this certificate?	Select Yes or No . Yes will enable Trust Protection Platform to turn on daily TLS validation of this certificate.
Port	The network port that Trust Protection Platform will use to connect to the target device hosting the certificate when making the TLS connection.
Use certificate's Common Name	Validation scans include network addresses resolved from the common name of the certificate.
Use certificate's DNS Subject Alternative Names	Validation scans include network addresses resolved from the DNS Subject Alternative Names (SANs) of the certificate, if any.
Validate the chain returned by the hosting server	The chain returned by the hosting server is compared to the chain that Trust Protection Platform builds using its internal algorithm to ensure a match. By default, chain validation is enabled and affects the SSL/TLS validation result.
Advanced Settings	
Managed By	Choose Aperture if the policy is managed by that application. If not, leave this field blank.
Certificate Origin	The friendly name of the system requesting the certificate. Used for reporting purposes only. (Requires Client Protect product.)
CSR Signature Algorithm	Choose either SHA-256, SHA-384, or SHA-512. The default is SHA-256. To learn more about signing algorithms, see About signing algorithms .
Generate Key/CSR Remotely	Option to enable the remote generation of the key or CSR on the HSM (requires Venafi Advanced Key Protect). When one or more of the following items are true, Remote Generation is not supported and, therefore, this setting is ignored: You're using a driver that does not support remote generation.

Field	Description
	To learn which drivers support remote generation, see Supported integrations: devices, applications, services and features supported by Venafi. - You're using a self-signed CA template to enroll a certificate; self-signed CA templates do not work with remote generation. This is because Trust Protection Platform requires that the private key be stored centrally so that it can be used to sign the self-signed certificate. - Your certificate is associated with more than one application; to work correctly, the certificate must be associated with <i>one</i> application. - You have not set the certificate's management type setting to Provisioning.
Key Generation and Encryption Key	Encryption key used to generate the certificate's private key. Trust Protection Platform provides either an AES-256 software encryption key to generate private keys, or you can configure AES encryption keys stored on supported HSM devices to generate certificate private keys. For information on using your own encryption keys, see Managing system credentials
Allowed Domains	Enter the suffix of allowed domains. <i>Example: acme.com or sales.acme.com</i> If you leave this field blank, ALL domains will be allowed.
Allow wildcard Common and Subject Alternative Name	Select to allow wildcards in the certificate's Common or Subject Alternative Names.

Field	Description
Allow duplicate Common and Subject Alternate Names	Select to allow duplicate Common or Subject Alternate Names. To learn more, see "About Subject Alternative Names (SANs)" on page 174.
Disable "Certificate Download Password" Complexity	The setting allows an administrator to revert back to the previous functionality where a password is required but there are no length or complexity requirements. If this check box is not selected, the password requirements are: ◦ Password is at least 12 characters. ◦ Comprised of at least three of the following: • Uppercase alphabetic letters • Lowercase alphabetic letters • Numeric characters • Special characters

Field	Description
Private Key PBE (password-based encryption) Algorithm	This setting applies only to PKCS#8-formatted private keys downloaded from Aperture, WebAdmin, or WebSDK. Choose the type of algorithm appropriate for your environment. To learn more about PBE algorithms, see "Using PBE (password-based encryption) algorithms to secure private keys" on page 329. NOTE The algorithms used to derive the protection key and encrypt the private key are not supported by all applications. Generally, the more secure the protection key and algorithm, the fewer applications will support it.
SAN Types Allowed	This allows you to control the SAN types that are allowed or not allowed for certificate enrollment. The available SAN types that can be controlled by policy are: ◦ DNS ◦ IP ◦ UPN ◦ Email ◦ URI If your system was installed with version 18.2 or older of Trust Protection Platform, all SAN types are allowed by default. If your first installation of Venafi Platform was version 18.3 or later, only DNS SAN types are allowed by default. Use this control to determine which SAN types you want to permit at this and lower folder levels.

About a certificate's summary (Policy Tree)

The **Certificate > Summary** tab provides a snapshot of the current certificate. It lists the certificate status, all associated applications, the certificate signature chain, and the certificate details.

NOTE Any user with *Write* permission to the certificate can access all of the options in the Certificate Summary tab and view all summary data, including information about the certificate's associated applications regardless of whether the user has permissions to the associated applications.

Certificate Status section

The Certificate Status section contains detailed information about errors, processing, validation, and other vital details.

(Status messages) Just below the Certificate Status title bar, Trust Protection Platform displays the current status of the certificate object, including the following common messages:



There is no processing and the certificate is working.



The certificate is being processed. The status field provides a description of what is happening.



There is a problem and the certificate is not functioning. The status field provides a description of the problem.



Workflow request has been rejected.

Expiration Date

States the date and time that the certificate will expire. A value will be shown only if the certificate object has a certificate currently linked to it.

Lifecycle Stage

Processing Stage states the stage number that the certificate is currently on. Certificate will state "none" if it is not currently processing.

Revocation

Shows the date and time of the last revocation check, as well as the result of the last revocation check.

Validation

Displays the time stamp for the last network validation of the certificate. Network validation settings are controlled on the Validation tab of the certificate object.

Displays the results of the last network validation attempt for the certificate object.

Associated Applications

This section lists the applications the certificate object is associated with. It also details the current status, processing stage, and validation results of each specific associated application.

Certification Path

If a certificate is currently linked to a certificate object, Trust Protection Platform will build the root chain for the certificate and display it here.

Certificate Details

Trust Protection Platform lists all of the details of the certificate that is linked to the certificate object. All the details of each certificate in the root chain are displayed here as well.

About Viewing Certificate History

You can view certificate history to see previous versions of a certificate that has been renewed.

When you are viewing a certificate, you can open the **Previous Versions** page to see a list of previous versions of the certificate that have been replaced.

102.generated.venafi.com

Policy\Generated\Certificate 100 - 199

Overview

Installations

SSL/TLS

Previous Versions

Permissions

This list shows previous versions of the certificate which have been replaced.

Displaying 2 Previous Certificates

Common Name	Serial Number	Issuer	Valid From	Valid To	Status	
102.generated.venafi.com	1E0CB92EC0942448BB3EF92FCCA324AD	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download
102.generated.venafi.com	0DD61A394451AC4497B4A2D56857C1B6	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download

For each item in the list you can see selected information about the certificate. For complete certificate details, click on the certificate **Serial Number**.

For more details on working with historical certificates see:

- "Revoke historical certificates" on page 314
- "Revert historical certificates" on page 315
- "Download historical certificates" on page 316

Configuring certificate settings via policy

When a system object is defined under a Policy object in Policy Tree, the object and its corresponding resource are associated with the policy and are subject to the policy settings. For example, if you configured the certificate management type in a Policy object, Trust Protection Platform would read those values for the policy's subordinate Certificate objects. Thus, policies can be used to standardize object configuration parameters and enforce security requirements.

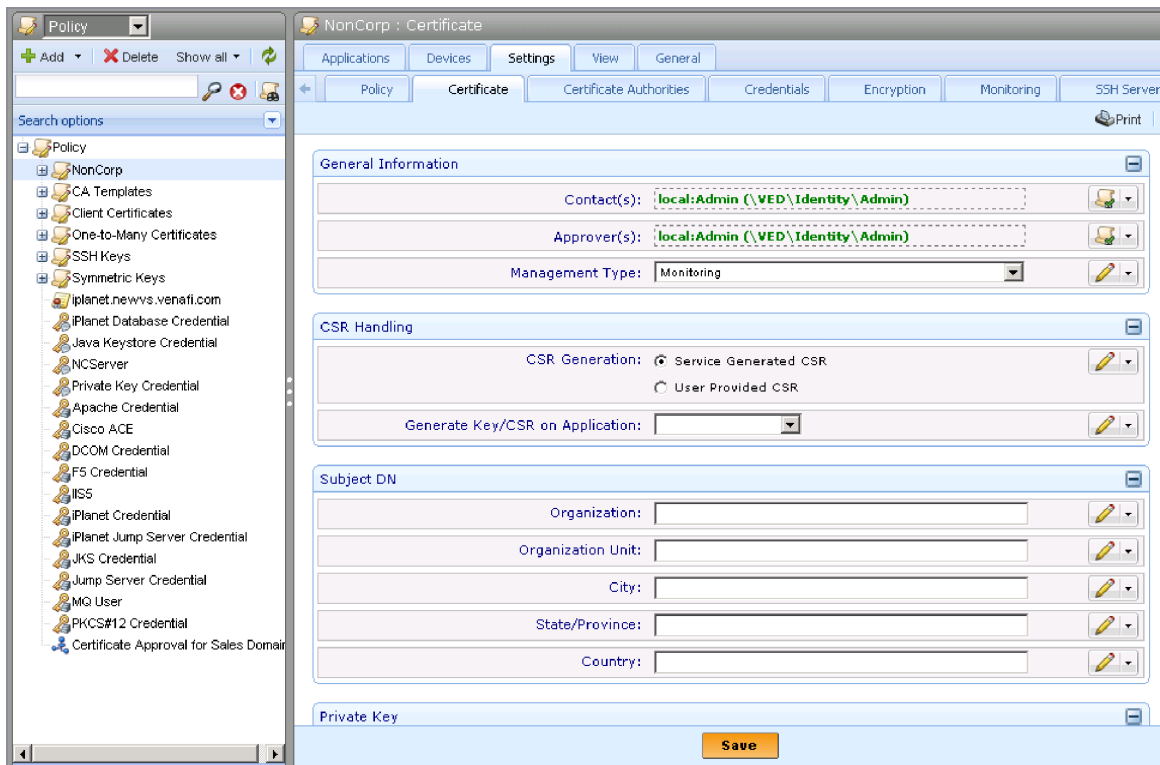
For more detailed information on how folders work, see [Using policies to manage encryption assets](#) of the *Venafi Trust Protection Platform Administration Guide*.

You must have *Write* permissions on the Policy object where you want to configure the certificate settings.

To configure the certificate settings in the Policy object

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. In the Policy tree, select the Policy object where you want to configure certificate settings, and then click the **Settings** tab.

The Detail View displays the Policy object's associated settings.



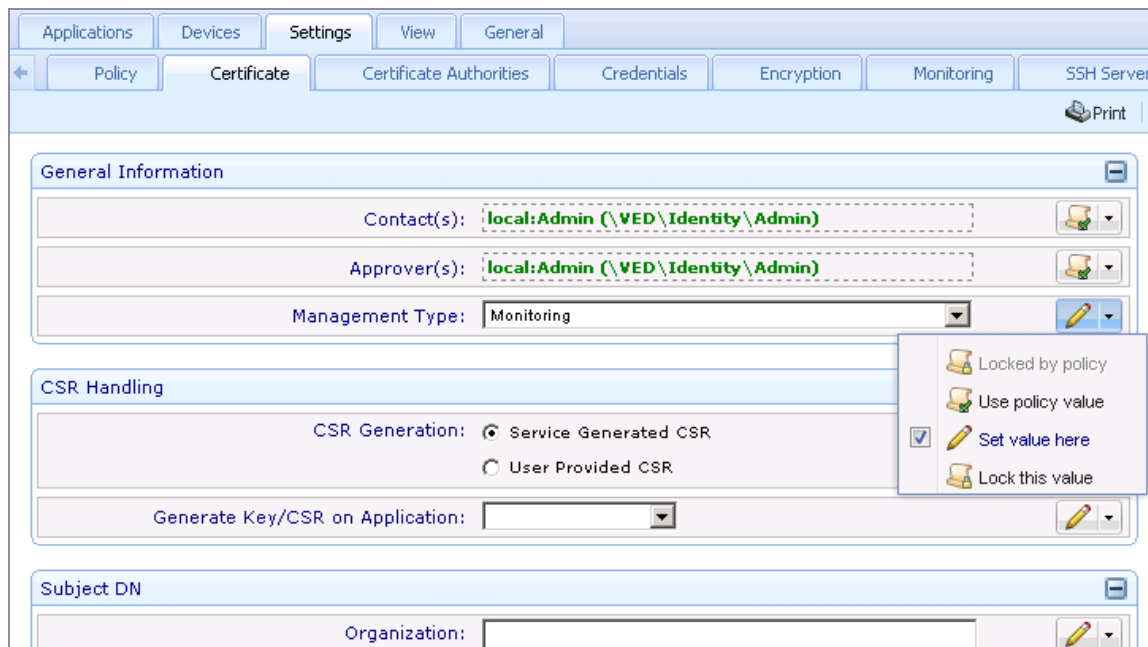
3. There are two Policy configurations for Certificate objects: the Certificate and Monitoring tabs. The following sections outline these configuration options:
 - "Policy object certificate settings" on page 319
 - "Policy object monitoring settings" on page 327
4. To learn about configuring settings for certificates in Policy Tree, see "About certificate object settings" on page 146.
5. To learn about configuring settings for certificates in Aperture, see "Setting policy on a folder" on page 177.
6. Lock or unlock the value.

When you define an attribute within a Policy object, 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 .

7. To lock a policy value in Policy Tree, click the attribute's drop-down menu .

The menu shows the available options for the current attribute.



8. Click **Lock this value**.

The attribute's icon changes to indicate the current value is in a locked state .

9. To lock a policy value in Policy Tree, click the **Unlocked** icon .

The value toggles between a locked  and unlocked  state.

10. When finished, click **Save/Apply**.

Policy object certificate settings

A policy object Certificate tab allows you to define settings, such as the certificate management type, for the subordinate certificate objects.

Certificate settings defined for a folder take precedence over the settings defined in the subordinate certificate objects *if* the values are locked. Otherwise, the policy's certificate settings function as default values for subordinate certificate objects.

The following table describes Policy Tree Policy object **Settings > Certificate** tab.

Field	Description
Certificate Tab	The Certificate tab defines certificate settings for subordinate certificate objects. Certificate settings defined at the folder level may take precedence over those defined in the subordinate Certificate objects. TIP The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the channel and notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393.
General Information	
Contacts	User or group identities assigned to subordinate certificate objects. Default system notifications are sent to the contact identities.
Approvers	User or group Identities assigned to approve workflows (certificate approval or injection command) for subordinate Certificate objects. For more information on defining Workflows, see "Implementing certificate workflow management" on page 557 . For information on when Trust Protection Platform references approvers defined in the Certificate object, see the option "Approver Assigned to Object" on page 571 .
Management Type	Level where subordinate certificates will be managed. The default is Provisioning. Trust Protection Platform provides the following levels of certificate management: ▪ Monitoring: Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform notifies the administrator. It does not, however, renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then retrieve and install the renewed certificate.

Field	Description
	▪ Enrollment: Trust Protection Platform can automatically generate and submit CSRs to Certificate Authorities using the parameters defined in designated CA Template objects. If preferred, the administrator can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the central database. The administrator must then download the certificate from Trust Protection Platform and install it on the target systems. ▪ Provisioning: Trust Protection Platform manages the entire certificate lifecycle—it automatically requests, installs, and monitors your system 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.
Managed by	The Venafi application that manages the policy. Choose Aperture or User Portal if the policy is managed by that application. If not, leave this field blank.

CSR Handling

CSR Generation	Determines how CSRs are generated. The default is Service Generated CSR: ▪ Service Generated CSR: Trust Protection Platform automatically generates the CSR. ▪ User Provided CSR: CSR is manually generated by the administrator, then uploaded to Trust Protection Platform.
Generate Key/CSR on Application	Determines where the CSR and private key are generated. The default is No. IMPORTANT When one or more of the following items are true, Remote Generation is <i>not</i> supported and, therefore, the <i>Generate Key/CSR on Application</i> setting is ignored. ▪ You're using a driver that does not support remote generation.

Field	Description
	To learn which drivers support remote generation, see Supported integrations: devices, applications, services and features supported by Venafi. ■ You're using a self-signed CA template to enroll a certificate; self-signed CA templates do not work with remote generation. This is because Trust Protection Platform requires that the private key be stored centrally so that it can be used to sign the self-signed certificate. ■ Your certificate is associated with more than one application; to work correctly, the certificate must be associated with <i>one</i> application. ■ You have not set the certificate's management type setting to Provisioning. ■ You're doing one-to-many provisioning. If you do not select this option, the CSR and private key are centrally generated on the Trust Protection Platform server, then securely copied to the application. If you do select this option, the CSR and private key are locally generated on the application's server. In both cases, the certificate and private key are archived in the Trust Protection Platform database.
Hash Algorithm	For the certificate signing request, choose either SHA-256 , SHA-384 , or SHA-512 . The default is SHA-256.
Subject DN	
Organization	Name that uniquely identifies the organization in the certificate.
Organization Unit	Department or division within the organization that is responsible for maintaining the certificate.

Field	Description
City, State/Province, Country	Location (city, state/province, and country) of your Organization or Organizational Unit.

Domain White List

Allowed Domains	Enter the suffix of allowed domains. For example, <i>.com</i> <i>acme.com</i> , or <i>sales.acme.com</i> . If you leave this field blank, all domains will be allowed.
Allow Wildcards	The default is Yes . Select No to prohibit wildcards.
Allow Duplicate Common and Subject Alternate Names	The default is Yes . Select No to require unique names.

Private Key

Reuse Private Key for Service Generated CSRs	Reuses the original private key when renewing the certificate. The default is No.
Allow Users to Import Duplicate Certificates and Reuse Private Keys	Controls the reuse of certificates and private keys. When enabled, this permits you to import a certificate even if another certificate with the same private key already exists in the system. It would also allow you to renew a certificate without uploading / re-generating a new private key. When disabled, if you are renewing a certificate with a user-provided CSR, you cannot reuse a CSR that is tied to a private key that has ever been uploaded to Trust Protection Platform. Also, when importing a certificate manually, through WebSDK and Web UI, you won't be able to upload a certificate that is already in the inventory. We recommend you leave this option disabled (unchecked).

Field	Description
	NOTE If you enable this option, you must have Write permission for the original certificate. Failing to have this permission will result in the system producing an error message: Duplicate Certificate. Insufficient Permissions to View Existing Certificate.
Allowed Algorithms	Dictates which algorithms can be used within the scope of the policy. Administrators can use the controls in the UI to add and remove allowed algorithms. To see a list of supported algorithm types, see Algorithm types supported by Venafi Platform. To learn more about algorithms, see Understanding cryptographic algorithms in Venafi Trust Protection Platform.
Default Algorithm	Sets an algorithm (chosen from the allowed list) to use when a certificate doesn't specify one. Administrators can use the controls in the UI to make sure that a default is always in place. The Use System Default option means to use whatever algorithm is currently selected as the default for that policy. This setting has its own policy control, which can be set on a per-policy basis. If none are set, it falls back to the global default list configured in VCC.s
Other Information	
CA Template	CA Template object that reTrust Protection Platformferences to generate the CSR and submit it to the CA.
Key Generation	Encryption key to generate the certificate private key. By default, Trust Protection Platform provides an AES-256 encryption key—the Venafi Platform software key—to generate private keys. However, you can also configure Trust Protection Platform to use AES encryption keys stored on supported HSM devices to generate certificate private keys. Your system is protected by either a hardware or a software encryption key (or both).
Encryption Key	Encryption key to use to protect the certificate private key.

Field	Description
	The system uses either a hardware or software key (or both). The software encryption key secures data in the Trust Protection Platform database, and is stored in the Windows registry. You can also configure Trust Protection Platform to use AES encryption keys stored on supported HSM devices to encrypt your system certificates. For information, see Managing system encryption keys in the <i>Trust Protection Platform Administration Guide</i>.
Disable Automatic Renewal:	Disables enrollment and provisioning for the current certificate. This means that Venafi TLS Protect does not attempt to renew or install the current certificate. However, Venafi TLS Protect still provides monitoring, validation, and notification for the certificate object. Additionally, the certificate is represented in Dashboard statistics and system reports. The default is No. Trust Protection Platform automatically selects this option when it renews a certificate in response to a SCEP request.
Allow Simple Passwords for Private Key Downloads	The setting to control whether simple or strong passwords are required for private key downloads. The default is No.
PKCS#12 Encryption Algorithm	Each algorithm has its own security and compatibility level. Generally, higher security means lower compatibility with software applications.
Private Key PBE (password-based encryption) algorithm	This setting applies to private keys that are downloaded using the PEM format. Options include: Insecure but good system compatibility, Insecure but better system compatibility (SHA1 3DES), High security but low system compatibility (SHA256 AES256). The default is <i>High security but low system compatibility (SHA256 AES256)</i>. You should not change it unless you have an incompatible system that cannot be upgraded.

Field	Description
	For more information, see "Using PBE (password-based encryption) algorithms to secure private keys" on page 329.
	NOTE The algorithms used to derive the protection key and encrypt the private key are not supported by all applications. Generally, the more secure the protection key and algorithm, the fewer applications will support it.
Renewal Window	Number of days prior to expiration that Trust Protection Platform begins the renewal operation. The default and recommended value is 30 days.
Validation	The purpose of Network Validation is to confirm that the certificate is functional and to verify that the correct certificate is being used. Network Validation requires network access to the server where the application is installed.
Disable SSL/TLS Validation	Disables Network Validation, including all related notifications, for subordinate Certificate objects.
Network Port	Port that the Validation Manager uses to connect to the server where the application is installed. The Validation Manager uses an SSL connection to validate the application's associated certificate. The default port is 443.
Use certificate's Common Name	Require validation scans to use a DNS lookup to resolve the certificate Common Name. Validation occurs on the certificate at every IP address returned from the DNS lookup. The default is Yes.
Use certificate's DNS Subject Alternative Names	Require validation scans to validate DNS Subject Alternative Names (SANs) of the certificate, if any. The default is No.

Field	Description
Validate the chain returned by the hosting server	Validate the chain returned by the hosting server to the chain that Trust Protection Platform builds using its internal algorithm to ensure a match. The default is yes, meaning chain validation is enabled and it affects the SSL/TLS validation result.
Approved Certificate Authorities	Available only in the Root Policy object.
Approved for Issuance	Available only in the Root Policy object. Select certificate authorities (CAs) you want to be considered trusted and approved issuers. This list is useful in identifying certificates issued by unapproved CAs. You can configure the Critical Alerts widget in the product dashboard to identify certificates that do not match your approved CA list.
Active Directory Certificate Authentication	Device, user, server, and certificates policy settings related to Active Directory certification authentication and SID (security identifier).
Allow certificates with AD Security Identifier (SID)	The default is No. If set to No, Trust Protection Platform will not allow certificates with an SID extension.

Field	Description
Allow security identifiers outside of connected identities	The default is No. Controls whether Trust Protection Platform allows unknown SID (security identifier). If set to No and Trust Protection Platform cannot find the provided SID value in AD, the certificate request is rejected.
Automatically include requester identity	The default is Yes. Applies to WebSDK. If set to Yes, the WebSDK requester identity is set as the AD security identifier (SID) identity, unless provided with the request. If Trust Protection Platform cannot resolve objectSid from the WebSDK requester identity, it is ignored. If the resolved SID value doesn't match the policy settings, then the request is rejected.
AD Security Identifier source	Choose between: - Look up SID from AD Identity. Resolves SID from the provided AD identity. - Enter SID manually. Manually-specified SID. Supports macros. Main use case for macros is to set a setting on a policy and lock it. If a macro is provided with the request, the Allow security identifiers outside of connected identities setting must be set to Yes.

Policy object monitoring settings

The policy object's Monitoring page allows you to define the intervals at which Trust Protection Platform generates expiration events for the Policy object's subordinate Certificate objects.

The following table describes the options in the Policy Object's **Settings > Monitoring** tab:

Field	Description
Monitoring Tab	The Monitoring tab defines the expiration event settings for subordinate objects—you can define how soon and how often expiration events are generated for the policy's subordinate Certificate objects. Monitoring parameters defined in folder may take precedence over the monitoring parameters defined in the Certificate objects. The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the Channel and Notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393 in the Certificate Management guide.
Expiration Start	Number of days before a certificate expires that you want to start generating expiration events.
Expiration Interval	Frequency (in days) at which you want Trust Protection Platform to generate expiration events.
Escalation Start	Number of days before a certificate expires that you want to start generating escalated expiration events.

Field	Description
Escalation Interval	Frequency (in days) at which you want Trust Protection Platform to generate escalated expiration events.
Disabled	Disables Monitoring for all subordinate Certificate objects.
Policy	Allows you to lock a value within the Policy object. Locked attributes cannot be modified in subordinate Certificate objects. Unlocked attributes function as suggested values; they can be accepted or overwritten in the subordinate object configuration. By default, policy values are unlocked . The value toggles between a locked  and unlocked  state. The first Policy icon locks or unlocks the Expiration Start values. The second Policy icon locks or unlocks the Escalation Start values. The third Policy icon locks or unlocks the Disabled value.

Determining certificate compliance

The **Compliance** tab provides an assessment of the certificate's compliance with its parent folder.

- The Certificate Value column lists the certificate values as they are currently defined in the certificate. Certificate Values are listed as being in  or out  of policy.
- The Renewal Value column lists the certificate values currently defined in the Certificate object. Renewal values also reflect policy status.

The screenshot shows a web interface for managing certificates. The main window is titled 'cert : Compliance'. It has a navigation bar with tabs: Certificate, Monitoring, Validation, and General. Below the navigation bar are icons for Summary, Settings, Associations, Compliance (selected), and History. A 'Print' button is also visible.

The 'Compliance' tab is active, displaying a form for 'Subject DN & Key Strength'. This form has two columns: 'CERTIFICATE VALUE' and 'RENEWAL VALUE'. The fields are as follows:

	CERTIFICATE VALUE	RENEWAL VALUE
Common Name:	cert	cert
Subject Alt Name (DNS):		
Organization:		
Organization Unit:		
City:		
State:	Utah	Utah
Country:	US	US
Key Strength (bits):	1024	

Below the 'Subject DN & Key Strength' section is the 'Other Information' section, which contains the following details:

- Certificate Authority: VenQA CA
- Public Key Algorithm: rsaEncryption
- Signature Algorithm: sha1RSA

Associating certificates with applications

To enable Venafi Trust Protection Platform™ to manage one or more certificates on a platform or keystore, you must associate the Application object with the corresponding Certificate object(s). When you associate an Application object with a certificate and enable processing, Trust Protection Platform manages the certificate and private key on the server where the application resides.

Depending on the level of certificate management configured on the certificate—Monitoring, Enrollment, or Provisioning—Trust Protection Platform may perform the following actions on the applications associated with a certificate:

- If you associate an existing certificate with an application where the certificate is not currently installed and Provisioning is enabled, Trust Protection Platform installs the certificate and private key on the application's server, overwriting the existing certificate and private key.

- If the certificate does not yet exist and Enrollment or Provisioning is enabled, Trust Protection Platform generates the key pair and CSR (either on the application's local server or on the Trust Protection Platform server as determined by the Certificate object configuration), submits the CSR to the CA, then retrieves the certificate. If Provisioning is enabled, Trust Protection Platform also installs the certificate and private key on the target platform or keystore.
- If the certificate already exists on the application's server and Monitoring is enabled, Trust Protection Platform monitors the certificate lifecycle and provides notification when the certificate is about to expire. If Provisioning is enabled, Trust Protection Platform replaces the certificate when it expires using the parameters defined in the Certificate object and/or its associated policy.

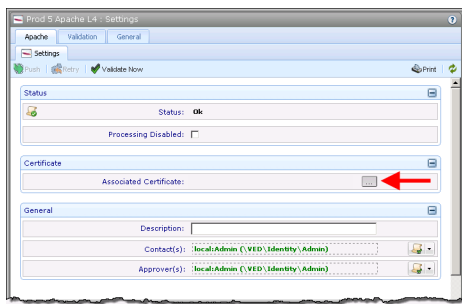
You can associate certificates with applications from either the Certificate or Application object configurations.

Associating a certificate with an application object

Before you can associate a certificate with an application, you must have *write* permissions to the application object and either *write* or both *associate* and *view* permissions to the Certificate object.

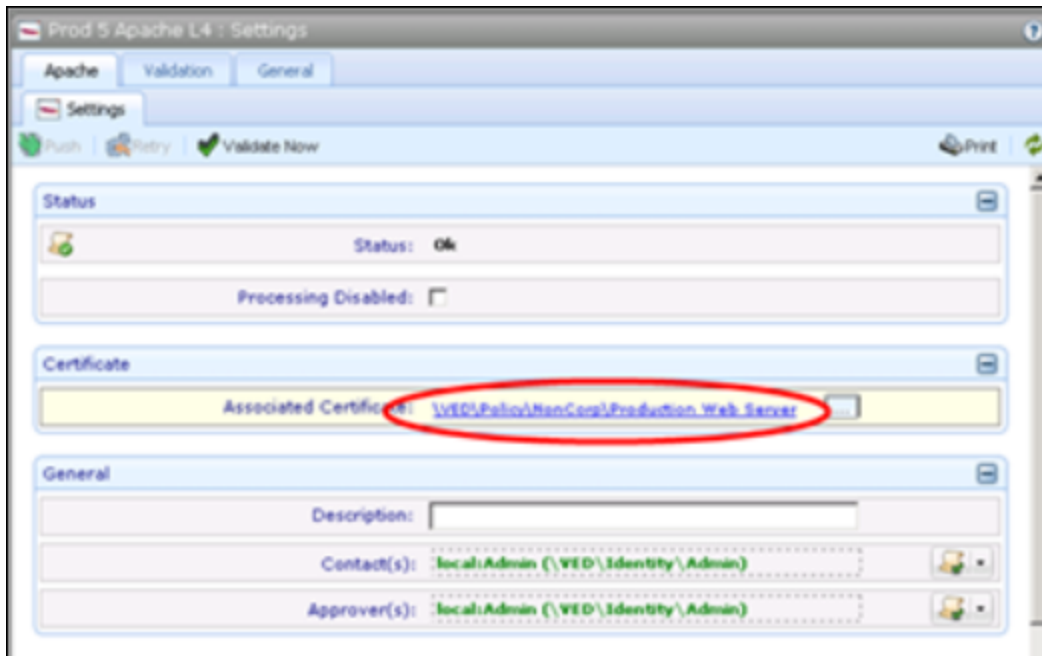
To associate a certificate with an application object from the application object

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. In the Policy tree, select the Application object you want to associate with a certificate.
3. Select the **Settings** tab.



4. In the Associated Certificate field, click the Browse button.
5. The Certificate Selector dialog opens.
6. Select the Certificate object you want to associate with the application, and then click **Select**.

The Certificate object is associated with the current application.



Certificate Object Associations options

The following table reviews the options found on the application object's **Settings** tab.

For more detailed information about application object configuration, see [Managing applications](#).

Option	Description
 Push	Pushes the application's associated certificate and private key to the current application. IMPORTANT You must have Write permissions to the Application object and either Write or Associate permissions to the Certificate object to push the certificate 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 will 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. ▪ You must have either Write or Associate permissions to the associated Certificate object. ▪ You must have Write permissions to the current Application object.
 Retry Installation	Reattempts to install the associated certificate on the current application. IMPORTANT You must have Write permissions to the Application object and either Write or Associate permissions to the Certificate object to install the certificate on the selected application.

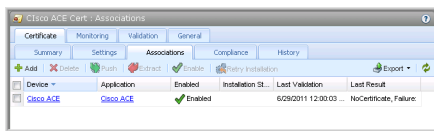
Option	Description
 Validate Now	Queues the validation request with the Validation Monitor engine. When the Validation Manager executes the validation scan, it runs the validation check on the current application and its associated certificate according to the settings configured in the Application object's Validation tab. The results are shown in the Validation tab and Trust Protection Platform generates the corresponding validation events. For more information on application object validation, see About certificate and application validation.
 Export	Exports the Application's configuration data to a CSV, tab-delimited, HTML, or XML file.
 Refresh	Refreshes the contents of the current page.

Associating a certificate with an application from the certificate object

You must have *Write* permissions to the Certificate object and either *Write* or both *Associate* and *Read* permissions to the Application object before you can associate certificates with an application object.

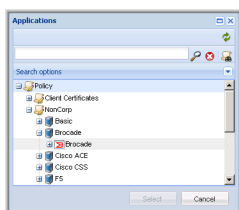
To associate a certificate with an application from the certificate object

1. From the [TLS Protect menu bar](#), click [Policy Tree](#).
2. In the Policy tree, select the Certificate object you want to associate with the application, and then click the **Associations** tab.



3. In the Details view, click **Add**.

The Applications Selector dialog opens.

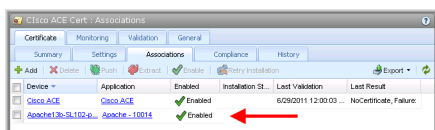


- Expand the parent Device object, then select the Application object you want to associate with the certificate.

You must have either Write or both Associate and View permissions to the Application object to select it in the Applications Selector dialog.

- Click **Select**.

The Application object is added to the certificate's list of associated applications.



- Repeat the previous three steps for every application you want to associate with the certificate.

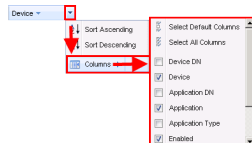
For more information on one-to-many configurations, see ["Associating certificates with multiple applications \(one-to-many\)"](#) on page 211.

Certificate object associations options

The following table reviews the options available on the **Associations** tab.

Option	Description
Column Sort	To sort the list by a particular column, click on the column heading. The sort toggles between ascending and descending order. NOTE In Policy Tree, the column sort order is stored in the administrator's User object. Therefore, Policy Tree always reflects the user's most recent column sort order, even if the administrator logs in from another workstation. In Policy Tree, the column sort order is reset every time you log in unless you bookmark the page. When you bookmark the page, the column sort order is saved and applied the next time you open that view. To bookmark the page, define the column sort order, and then click the share icon.
Columns	Determines the columns that display on the Certificate Associations tab. NOTE In Policy Tree, the column settings are stored in the administrator's User object. Therefore, Policy Tree always reflects the user's most recent column settings, even if the administrator logs in from another workstation. In Policy Tree, the column settings are reset every time you log in. To access the Column menu in Policy Tree Click the drop-down menu icon for a given column. Click Columns.

Columns {3} From the Columns menu, you can select the columns that you want to display in the Discovery Results tab.



To access the Column menu in Policy Tree, right-click any column heading, then select the columns that you want to display in the Discovery Results tab.

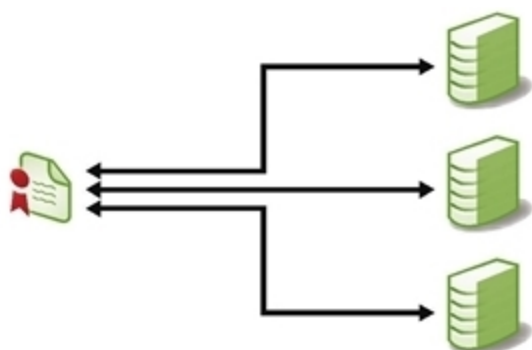
Option	Description
	Add Associates an Application object with the current certificate. IMPORTANT You must have Write permissions to the Certificate object and either Write or both Associate and Read permissions to the Application object to associate an application with the current certificate. If you do not create a Network Certificate object below its associated Application object, Trust Protection Platform displays a Certificate Alias object below the associated Application object so you can see which certificates are associated with which applications. NOTE Alias objects are hidden by default. To view Alias objects in the Policy tree, you must enable the Show Aliases option. In the Windows console, click File > Preferences > Policy Tree, then select Show Aliases. In Policy Tree, click Show All > Show Aliases.
	Delete Disassociates the selected Application object from the certificate. IMPORTANT You must have Write permissions to the Certificate object and either Write or both Associate and Read permissions to the Application object to disassociate it from the current certificate. This option does not delete the Application object from the Policy tree or remove the certificate from the application's server.
	Push Pushes the current certificate and private key to the selected application. IMPORTANT You must have <i>Write</i> or <i>Private Key Write</i> permissions to the Certificate object and either <i>Write</i> or both <i>Associate</i> and <i>Read</i> permissions to the Application object to push the certificate 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.

Option	Description
	Trust Protection Platform will 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. ▪ You must have Write permissions to the current Certificate object. ▪ You must have either Write or Associate and Read permissions to the selected Application object.
	Extract Extracts the certificate and private key installed on the selected Application objects. This option is available only in Policy Tree. IMPORTANT You must have <i>Private Key Write</i> and <i>Write</i> permissions to the Certificate object and both <i>Read</i> and <i>Private Key Read</i> permissions to the Application object to extract a certificate and private key from an application. 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. For more information, see "Extracting certificates and private keys" on page 213.
	Enable Toggles between enabling and disabling the processing of certificates on the selected application objects. When you disable processing, Trust Protection Platform does not attempt to install, renew, process, or validate certificates for the current application.
	Disable

Option	Description
	IMPORTANT You must have <i>Write</i> permissions to the Certificate object and either <i>Write</i> or both <i>Associate</i> and <i>Read</i> permissions to the Application object to enable or disable the certificate on the selected application.
 Retry Installation	Reattempts to install the certificate on the selected application(s). IMPORTANT You must have <i>Write</i> permissions to the Certificate object and either <i>Write</i> or both <i>Associate</i> and <i>Read</i> permissions to the Application object(s) to retry installing the certificate on the selected application(s).
 Export	Exports the Associations data to a CSV, tab-delimited, HTML, or XML file.
 Refresh	Refreshes the contents of the current page.

Associating certificates with multiple applications (one-to-many)

In many network environments, such as a multi-web server deployment supporting a corporate website, one certificate might be installed on multiple applications. This would be considered a *one-to-many* configuration.



Trust Protection Platform simplifies the distribution of certificates and private keys for one-to-many configurations. If you choose to associate multiple applications with one certificate on the certificate object's Associations tab, Trust Protection Platform can push the certificate and private key to the new servers. For more information, see "[Pushing Certificates and Private Keys to Applications](#)" on page 249.

IMPORTANT When one or more of the following items are true, Remote Generation is *not* supported and, therefore, the *Generate Key/CSR on Application* setting is ignored.

- You're using a driver that does not support remote generation.

To learn which drivers support remote generation, see [Supported integrations: devices, applications, services and features supported by Venafi](#).

- You're using a self-signed CA template to enroll a certificate; self-signed CA templates do not work with remote generation.

This is because Trust Protection Platform requires that the private key be stored centrally so that it can be used to sign the self-signed certificate.

- Your certificate is associated with more than one application; to work correctly, the certificate must be associated with *one* application.
- You have not set the certificate's management type setting to Provisioning.
- You're doing one-to-many provisioning.

If a certificate is already deployed on multiple servers, Trust Protection Platform can detect the configuration during a standard Network Discovery and bring the certificate and all its associated applications under management. During this process, Trust Protection Platform configures each unique instance of the certificate for validation and automatically creates a corresponding Basic Application object for each system where the certificate is installed. Each Basic Application object is automatically associated with the Certificate object and, if enabled, an Alias of the Certificate object appears under each Basic Application object.

Alias objects are hidden by default.

To view Alias objects in the Policy tree, you must enable the **Show Aliases** option.

To enable the Show Aliases option

1. From the [Platform menu bar](#), click **Policy Tree**.
2. In the Policy Tree menu in the left panel, click **Show all**.

3. Select **Show Aliases**.

To facilitate administration of one-to-many certificates, Trust Protection Platform tracks status and provides notifications for each certificate instance to ensure that administrators are aware of every affected server when a certificate fails.

For more information on bringing one-to-many certificates under management via Discovery, see ["Bringing network certificates under management"](#) on page 135.

Extracting certificates and private keys

Using the Policy Tree, Trust Protection Platform can extract certificates and private keys from applications associated with a certificate.

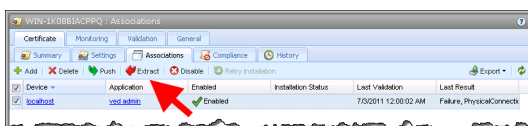
The Application associated with the certificate must be correctly configured for Trust Protection Platform to authenticate with the target application and find the certificate and private key file(s) in the application's local file system.

When you extract the certificate and private key, Trust Protection Platform encrypts the data, then archives the data in the Trust Protection Platform database so it can be distributed or downloaded on demand.

NOTE This option is available only in Policy Tree.

To extract a certificate and private key from an application associated with a Certificate

1. From the [Platform menu bar](#), click Policy Tree.
2. You must have Private Key Write and Write permissions to the Certificate object and both Read and Private Key Read permissions to the Application object to extract a certificate and private key from an application.
3. Select the **Policy** tree from the Tree drop-down menu.
4. In the Policy tree, select the Certificate object that you are going to extract the certificate and private key for.
5. Click the **Certificate > Associations** tab.



6. Select the application where you want to extract the certificate and private key.
7. Click **Extract**  .

IMPORTANT The Application object associated with the certificate must be correctly configured for Trust Protection Platform to authenticate with the target application and find the certificate and private key file(s) in the application's local file system.

8. If Trust Protection Platform has archived a certificate for the current Certificate object, Trust Protection Platform compares the extracted certificate and private key with the archived certificate. If there is a mismatch, Trust Protection Platform asks if you want to overwrite the current certificate and private key.
9. (Conditional) If prompted to overwrite the existing certificate and private key, verify the overwrite, and then click **OK**.

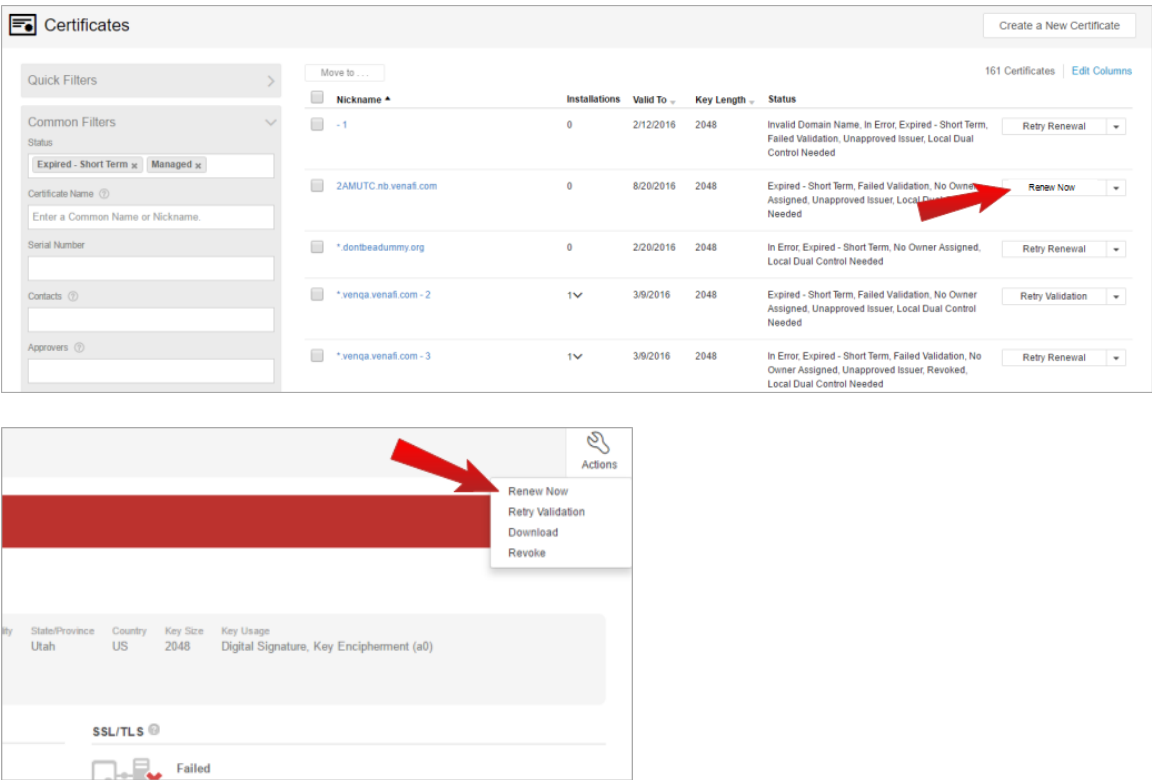
When finished, Trust Protection Platform notifies you that the certificate and private key were successfully extracted from the application. If there is an error during the extraction process, Trust Protection Platform indicates the nature of the error and aborts the extraction.

Renewing a certificate manually

The Renew Certificate wizard walks you through identifying the certificate and specifying its location.

To renew a certificate

1. Find the certificate you want to renew.
2. You can use filters to help narrow your search.
3. In the certificate list, click **Renew Now** or in the certificate's detail page, click **Actions > Renew Now**.



4. Review the Requested Renewal Details.

Requested Renewal Details

CERTIFICATE REQUEST DETAILS

Certificate Folder	Policy\North America
Nickname	cert-100-1024-SHA1-RSA-42-3
Management Type	Provisioning
Contacts	admin
Hash Algorithm	SHA-256
CSR Generation	Generate a CSR for me
Common Name	cert-100-1024-SHA1-RSA-42-3
Organization	Venafi
Key Strength	2048
Approvers	admin
Automatic Renewal?	No
Certificate Authority	Policy\North America\Eng\MCSA

5. Do one of the following:

- If no changes are needed, click **Renew**.
- If you need to make changes, click **Edit**, and then edit the Renewal Details.
- When you're done, click **Submit**.

In the certificate list, the state changes to **Renewing**.

Manually uploading the CSR

If you are managing a certificate under Enrollment or Provisioning, you have the option of manually generating the CSR, then uploading it to the Trust Protection Platform database so Trust Protection Platform can complete the enrollment process with the appropriate CA.

If the CSR is provided by a user, you might also want to upload the private key so it is archived in the Trust Protection Platform database. Trust Protection Platform must have a copy of the certificate's private key to provision certificates and key pairs. For more information, see ["Manually Uploading the Private Key" on page 218](#).

DID YOU KNOW? Why can't I specify SANs on my user-provided CSR?

Today, you can specify SANs on your CSR, but *only if the CSR has no embedded SANs*. Not all CAs support adding additional SANs (*additive SANs*); so to allow maximum compatibility across many CAs, Trust Protection Platform prevents the use of additive SANs.

To manually upload a CSR

1. From the [Platform menu bar](#), click Policy Tree.

You must have View and Write permissions to the Certificate object.

2. In the Policy tree, select the Certificate object whose certificate file you want to import.
3. Click the **Certificate > Settings** tab.
4. Click **Upload CSR**.
5. Do one of the following:
 - Paste the Base64-encoded CSR into the Paste window.
 - Click **Browse** to navigate the Directory structure, then upload a Base64 Binary-encoded CSR into Policy Tree.
6. Click **Upload**.

If **Service Generated CSR** is selected in the Certificate object configuration, then the uploaded CSR values are added only to the unlocked SubjectDN fields that are editable. No check is made to ensure that the values adhere to the Policy.

If **User Provided CSR** is selected in the Certificate object configuration, then the uploaded CSR values must adhere to the Policy before they are applied to the Certificate object. If they do adhere to Policy, they are added to the certificate and stored in the Trust Protection Platform database when the Certificate object is saved.

7. The uploaded CSR is securely stored in the Trust Protection Platform database and is used to renew the certificate.
8. When finished, click **Apply/Save**.

Manually Uploading the Private Key

When you create a new Certificate object, you have the option of uploading the private key so it is archived in the Trust Protection Platform database. The **Upload Private Key** option in the Certificate object allows you to paste the private key data or upload a private key file to the Trust Protection Platform database.

To manually upload a private key

1. From the SSH Protect menu, click **Configuration > Policy Tree**.

You must have the Private Key Write, View, and Write permissions to the Certificate object to upload a private key.

2. In the Policy tree, select the Certificate object whose certificate file you want to import.
3. Click the **Certificate > Settings** tab.
4. Click **Upload Private Key**.
5. Do one of the following:
 - Paste the Base64-encoded key into the Paste window.
 - Click **Browse** to navigate the Directory structure, then upload a Base64 Binary-encoded private key into the Policy Tree.
6. Enter the password required to access the private key.
7. Click **Upload**.
8. When finished, click **Apply/Save**.

When you upload the private key, Trust Protection Platform encrypts the data, then archives the key in the Trust Protection Platform database so it can be distributed or downloaded on demand.

About clearing certificate workflow errors

If there is an error at some stage of the certificate lifecycle and you manually resolve the problem—for example, if there is an error accessing a CA, so you manually submit the CSR—Trust Protection Platform does not know the problem has been resolved. Therefore, the workflow error remains and Trust Protection Platform cannot complete the certificate processing.

Trust Protection Platform TLS Protect provides three ways to clear certificate workflow errors:

- The  **Restart** option clears all errors and stages on the certificate and its associated applications, then restarts processing from the beginning.

This option is provided for circumstances in which the certificate or application was configured incorrectly. This option allows the administrator to restart the certificate processing so the correct information can be used. For example, if an administrator misspelled the certificate's common name, he or she could correct the spelling error, then restart the renewal process so the change is reflected in the new certificate. Restart can be used at any point during the renewal process

- The  **Retry** option clears the certificate error, then retries the last processing stage.

If the certificate is currently in an error state, this option clears the error, then queues the certificate to retry the current stage. For example, if a certificate was configured with an invalid CA template, the administrator could reconfigure the CA template, and then click **Retry** to resume the renewal process.

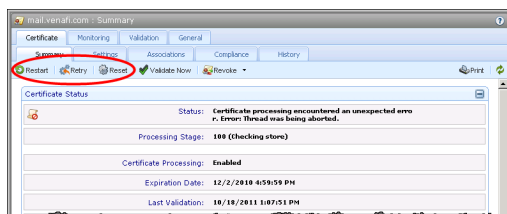
If there is an error on the certificate's associated application(s), then Trust Protection Platform reattempts to install the certificate on the associated application(s). Disabled applications are skipped.

- The  **Reset** option clear errors and stages on the certificate and its associated applications, then stop processing.

This option is provided for circumstances in which there is an error at some stage of the certificate lifecycle and the administrator decides to abort the current renewal process. For example, if a certificate completed the enrollment process, but failed when installing on one of the associated applications, the administrator could manually install the certificate on the application, and then click **Reset** to clear the error. In this instance, no further processing would be necessary.

In Policy Tree, the  **Restart**,  **Retry**, and  **Reset** options display at the top of the certificate

Summary page.



Clearing Certificate Workflow Errors

Before you can clear certificate workflow errors, make sure that you have *View* and *Write* permissions to the Certificate object.

To clear certificate workflow errors

1. From the **Platform menu bar**, click **Policy Tree**.
2. In the Policy tree, select the Certificate object where you want to clear the workflow errors.
3. Click the **Certificate > Summary** tab.
4. Depending on how you manually resolved the error, select one of the following options:
 - Click  **Restart** to clear all errors and stages on the certificate and its associated application(s), then restart processing from the beginning.
 - Click  **Fix > Restart Processing from the Beginning**.
 - Click  **Retry** to clear the certificate error, then retry the last processing stage.
 - Click  **Fix > Retry Last Failed Operation**.
 - Click  **Reset** to clear errors and stages on the certificate and its associated applications, then stop processing.
 - Click  **Fix > Reset Errors and Stop Operation**.

When you select one of these options, the certificate status changes accordingly on the Certificate Summary page.

About revoking certificates manually

You can manually revoke certificates that are managed at the Monitoring, Enrollment, or Provisioning level of certificate management.

NOTE You must have *write* and *revoke* permissions to the certificate object to revoke the certificate.

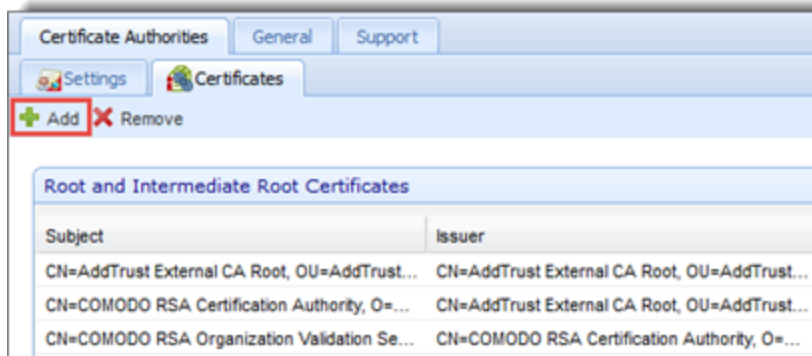
Manual revocation is supported by all CA drivers with the exception of the Self-Signed CA because revocation is only applicable to CA-signed certificates.

Revocation is generally limited to those certificates that were enrolled by Trust Protection Platform and those that belong to you and that were issued through your CA accounts.

When you revoke a certificate, Trust Protection Platform attempts to locate the corresponding certificate authority (CA) template object. If there is a CA template object which has a root or intermediate root which has the same name as the Issuer of the certificate being revoked, Trust Protection Platform attempts to revoke the certificate using that CA.

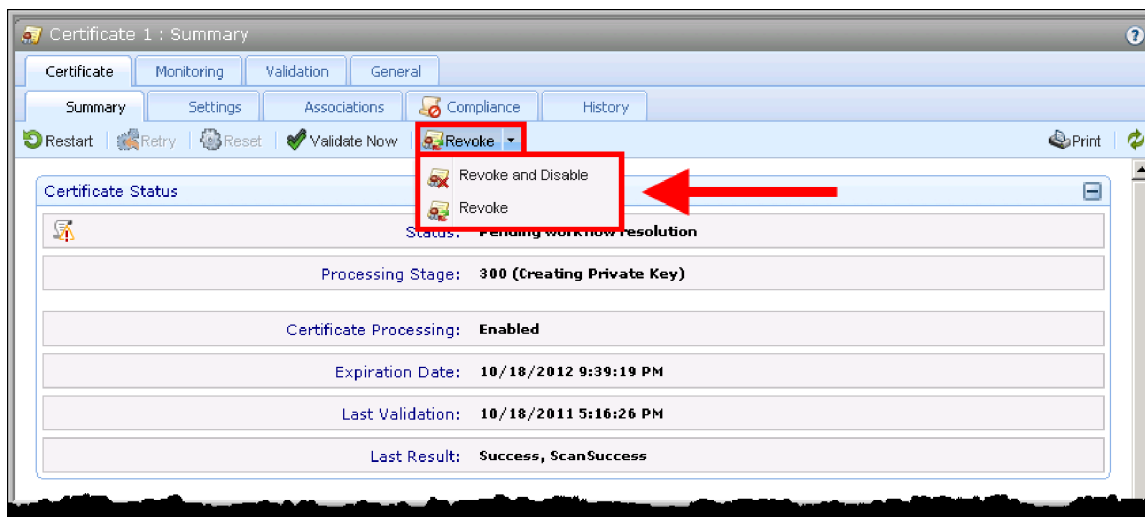
If more than one match is found, it attempts to use the first one located. If the issuer of the certificate is not found on any CA template object, it then attempts to revoke the certificate using the current CA configured on the certificate object.

To revoke a certificate dynamically, you must manually add intermediate or root certificates that issued your certificates to the corresponding CA template object.



If the Issuer of the certificate isn't known, Trust Protection Platform begins with the known CA and revokes the certificate based on the CA, not the Issuer.

The **Revoke** option is available in the certificate object's Summary and History pages. From the Certificate Summary page, you can revoke the most recent version of the certificate.



The **Revoke** option in the Certificate History page allows you to revoke previous versions of the current certificate that have not yet expired or been revoked.

For example, if you renew a certificate several months before it expires, you could provision the certificate on all of its associated servers then, after ensuring everything is functioning properly, you could revoke the previous, valid versions of the certificate in the Certificate History tab.

The **History** tab indicates the certificate(s) for which Trust Protection Platform has submitted a revocation request.

Common Name	Serial Number	Issuer	Valid From	Valid To	Status
79.mon1-5.venqa.venafi.c...	38B65193498FA73F602C...	CN=VeriSign Class 3 Sec...	10/16/2011	10/17/2012	Revoked
79.wed1-2.venqa.venafi.c...	3B496EFA00000000A1D7	CN=VenQA CA, DC=venq...	10/19/2011	12/03/2011	Valid
79.wed1-1.venqa.venafi.c...	3B48779A00000000A1D6	CN=VenQA CA, DC=venq...	10/19/2011	12/03/2011	Valid
79.wed1-0.venqa.venafi.c...	3B469F7E00000000A1D5	CN=VenQA CA, DC=venq...	10/19/2011	12/03/2011	Valid
79.tue1-0.venqa.venafi.com	3B2ACD4D00000000A1B5	CN=VenQA CA, DC=venq...	10/19/2011	12/03/2011	Valid
79.mon1-5.venqa.venafi.c...	31334D96000000005541	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Valid
79.mon1-4.venqa.venafi.c...	312FC0D500000000553F	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Valid
79.mon1-3.venqa.venafi.c...	312C17B300000000553E	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Valid
79.mon1-2.venqa.venafi.c...	30F1684300000000552D	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Revocation Pending
79.mon1-1.venqa.venafi.c...	30EF8DE5000000005529	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Revoked
79.mon1-0.venqa.venafi.c...	30A63CBB000000005519	CN=VenQA CA, DC=venq...	10/17/2011	12/01/2011	Revoked

When you revoke a certificate, Trust Protection Platform submits a revocation request to the certificate CA. If you select the **Revoke and Disable** option, Trust Protection Platform submits a revocation request to the certificate CA, and then disables the certificate so that no further processing can occur.

DID YOU KNOW? DigiCert CertCentral and GlobalSign MSSL do not support revocation from the History tab. This is due to behavior and restrictions that could result in unintentionally revoking other certificates.

To safeguard your system against unauthorized certificate revocations, you can configure a workflow to require approval for certificate revocations. Certificate revocations are assigned to stage 1400 of the certificate lifecycle, so you must configure the workflow to trigger on stage 1400. To implement the workflow, you must then apply the workflow in the appropriate folder. For more information on configuring and implementing Workflow objects, see [Workflow management](#).

When Trust Protection Platform processes a certificate revocation request, the revocation status appears in the Certificate Summary or History pages. Additionally, Trust Protection Platform logs the following events:

Action	Event
Request	The request to revoke <i>certificate_DN</i> has been submitted to the CA.
Success	The request to revoke <i>certificate_DN</i> has succeeded.
Fail	The request to revoke <i>certificate_DN</i> has failed.

The initial Revocation Request event can be viewed in the Certificate object's event log. The subsequent Success or Failure events can be viewed in the certificate's associated CA template object's event log.

For more information on object event logs, see [Log events](#) in the Log Server Administration Guide.

To facilitate management of revocation events, you can also create Notification objects to provide notifications of certificate revocation events.

For more information on configuring event notification, see ["About certificate notification and logging" on page 394](#).

Revoking a certificate

You can revoke a certificate from the certificate inventory or the certificate details page.

Move to ... 1410 Certificates [Edit Columns](#)

☐ Nickname ▾	Installations	Valid To ▾	Key Size ▾	Status	Last Renewed By	Valid From ▾	
☐ root agency	4 ▾	12/31/2039	512			5/28/1996	Download ▾
☐ fir.venafi.net.au	1 ▾	12/31/2037	2048			11/12/2015	Download ▾
☐ microsoft.root.authority	4 ▾	12/31/2020	2048			1/10/1997	Download ▾
☐ wmsvc-win-1k08biacppq	1 ▾	10/9/2020	2048			10/12/2010	Download ▾
☐ vdi-dev-dir-11	0	6/18/2020	1024			6/19/2015	Download ▾
☐ Duplicate 1	1 ▾	8/11/2019	2048			12/15/2016	Download ▾
☐ *.lds.org	1 ▾	4/17/2019	2048	Failed Revocation		1/9/2017	Retry Revocation ▾
☐ DESKTOP-19D7ARV	0	4/20/2018	2048			4/20/2017	Download ▾
☐ scepstestlab.venafi.com	1 ▾	3/14/2018	2048			3/14/2016	Download ▾
☐ 102.generated.venafi.com	23 ▾	2/6/2018	2048			12/7/2014	Download ▾
☐ Jared-PC	0	12/5/2017	2048			12/5/2016	Download ▾
☐ ahixson-dir1	0	12/1/2017	2048			12/1/2016	Download ▾
☐ ahixson-dir1a	0	12/1/2017	2048			12/1/2016	Download ▾

BEST PRACTICE It's a good idea to revoke certain certificates to prevent security breaches. For example, if an employee transfers to another department or leaves the company and has access to private key information for certain certificates, you should revoke those certificates and replace them.

To revoke a certificate

1. From the certificate list for the user you searched for, find the certificate you want to revoke.
2. Do one of the following:
 - From the certificate inventory, click **Revoke** on the action button.
 - From the certificate details page, click **Actions > Revoke**.
3. From the **Reason for Revocation** list, select a reason.

4. Click **Revoke** but remember, *this action cannot be undone*.

Revoke

Revoking this certificate will make it invalid. This action cannot be undone. If you decide later that the certificate is still needed, you will need to renew the certificate to request a new version that can be used.

Reason for Revocation
Unspecified

Comment

Common Name	Aaron Hixson
Organization	Venafi, Inc.
Organizational Units	Engineering
City/Locality	Salt Lake
State/Province	Utah
Country	US
Hash Algorithm	SHA-1
Has Private Key	Yes

Cancel Revoke

NOTE Revoking a certificate makes it invalid. The Certificate Authority is notified of this action.

Resolving problems for Revocations that resulted in a processing error

Revocations can fail for a number of reasons. The most common reasons revocations fail include:

- The revocation request was rejected by an approver
- The credentials to authenticate to the Certificate Authority were wrong
- Trust Protection Platform did not have the appropriate CA template configured for the CA that the certificate was issued from.

You can review the error message that will tell you why the revocation failed.

When Revocation fails, you have two choices:

- **Cancel.** Canceling a revocation means that even though it failed, you do not intend to retry revocation and you simply wish to clear the processing error from Trust Protection Platform. For example, you would do this in situations where the approver has rejected your request to revoke the certificate and you don't expect to receive approval on subsequent requests.
- **Retry.** Retry will clear the error and attempt revocation again. You should only do this after you have resolved the problem that caused the error in the first place. For example, if the revocation failed because the Certificate Authority credentials expired, you will need to ask your Administrator to update the credentials before you attempt revocation again. If it failed because it was rejected by approval, you will need to review the rejection reasons and retry after the approver's requirements have been met.

About Revocation Checking

This section provides an explanation of certificate revocation and how to use Venafi Trust Protection Platform™ to check the revocation status of certificates. Using Trust Protection Platform, you can verify the status of certificate revocations in the following ways:

- *Automatically*, by letting Trust Protection Platform check the revocation status on at least a daily basis and notify you when a certificate is found to be revoked. By default, automated checking occurs at least once per day. In the event that Trust Protection Platform discovers a revoked certificate, an automatic notification is sent to certificate owners, enabling them to take appropriate actions to avoid security issues.
- *Manually*, through the **Check Revocation Now** option. When you do a manual revocation check, Trust Protection Platform uses OCSP first, to try to verify the individual certificate being checked. If OCSP fails, Trust Protection Platform will check via the certificate's CDP.

Revocation checking is an important part of your PKI strategy for the following reasons:

- If you request that a certificate be revoked, you can verify that the CA took action to perform the revocation.
- When certificates are being added through Discovery, it is important to know whether or not the certificate is revoked, so you know what action to take on the certificate. For example, revoked certificates should not be in use any more, so it may not be worth the effort to try to identify their owners.
- If a revocation occurs outside Trust Protection Platform, you can be notified, and you can secure a new certificate for the affected systems. This is usually because a certificate owner in your organization is not aware of the process to revoke a certificate in Trust Protection Platform.

If a certificate is revoked, systems that rely on that certificate may incur an outage.

Revocation checking happens automatically as the CRL Distribution Points are verified by Trust Protection Platform. Every 24 hours, any certificate that could not be checked for revocation by the CDP, either because it is not tied to a CDP, or because the CDP was unavailable when checked, will be checked via OCSP to see if the certificate has been revoked.

NOTE Some CAs (for example, Let's Encrypt) do not use CRL Distribution Points at all and rely solely on OCSP for certificate revocation validation. Certificates from these CAs will only be checked automatically for revocation once per day.

IMPORTANT When a separate certificate from the CA (other than the issuing certificate of the certificate being checked) is signing the OCSP response, Trust Protection Platform requires it to have the OCSP key usage extension on the certificate.

About Certificate Revocation

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.

Certificate authorities (CAs) revoke certificates when they are no longer trustworthy. A certificate might be revoked for one or more of the following reasons:

- You are no longer using the certificate, so you submit a revocation request.
- The person or the computer to which the certificate was issued has been misidentified.
- The person or computer to whom the certificate was issued has lost the private key.

Revocation checking is a method used to inform relying parties (other individuals or computers) about compromised certificates. If a relying party checks the status of a certificate and finds that it is revoked, they should not perform any transactions using that revoked certificate.

CAs revoke certificates by placing them on a certificate revocation list (CRL). Many CAs issue CRLs every few days or even weeks, leaving trusted parties to unknowingly rely on outdated information. Between CRL updates, other parties continue to use the outdated CRL, considering its information to be valid when in fact a certificate they trust has been revoked since the last CRL update. Certificates that have been revoked and not yet replaced by a new, valid certificate can lead to system outages and downtime. This scenario can be avoided by ensuring that all parties are informed of the revocation so appropriate action can be taken.

Trust Protection Platform's Revocation Checking feature checks the revocation status of certificates in the Policy and Roots trees on at least a daily basis and sends notifications to administrators when a certificate is revoked. You can also force revocation status checking manually on individual certificates.

Supported Methods of Revocation Publication

Trust Protection Platform's Revocation Checking feature supports the following formats when retrieving CRLs from CDPs for automatic revocation checking:

- **CDP**. Monitored between 1-24 times per day. Also used as a backup for manual checks on certificates, if the OCSP check fails.
- **OCSP**. Used to immediately check a certificate's revocation status. Also used for once-daily checking of certificates that were not successfully checked using CDP during the previous 24 hours, or where CDP endpoints are not specified on the individual certificates.

You can enable or disable OCSP endpoints on the Roots tree in Policy Tree.

IMPORTANT OCSP endpoints are often reused on a CAs different intermediate roots. This means that you will see the same endpoint, for example "http://ocsp.digicert.com" under most of Digicert's intermediate roots. Disabling an OCSP endpoint will affect every certificate that uses that endpoint, even if they use different intermediate roots.

Trust Protection Platform expects all endpoints to be configured for anonymous authentication. When Trust Protection Platform is installed on a Windows server that is joined to a domain, Trust Protection Platform leverages the permissions of the account that VPlatform is running under if a FILE endpoint requires authentication.

Checking the revocation status of certificates

Trust Protection Platform automatically checks the revocation status of all enabled certificates in the inventory on a scheduled basis. You can configure this schedule as frequently as every hour, or as infrequently as once a day. If a certificate is found to be revoked, a notification will be sent to the contacts for the certificate and the status of the certificate will be updated. This keeps system administrators up to date on the status of their certificates in case they were aware of the revocation and need to update the revoked certificate with a new one.

Trust Protection Platform also provides the option to check the revocation status of an individual certificate at any time. Manually checking revocation is useful when you want to confirm that a revoked certificate is actually on the currently published CRL or even suspect that a specific certificate has been revoked without the appropriate approvals.

NOTE Manual checking of a certificate only checks the current version of the certificate. Trust Protection Platform checks any certificates found on the **History** tab of enabled certificates (that have not expired or been revoked) during the scheduled revocation check.

You can also view the revocation status of all certificates within a policy object from that object's **View > Certificate** tabs.

How it works

Revocation checking uses a combination of CRL Distribution Points and OCSP endpoints to gather its information.

1. CRL Distribution points are downloaded per the schedule configured on the Platform tree in Policy Tree, on a schedule ranging from daily to hourly.
2. When a CRL is downloaded it is digitally verified and all serial numbers that appear on the list are cross-checked with certificates that are in the certificate inventory.

Any certificates that are found on the CRL are marked as *Revoked* in the certificate inventory.

3. During the processing of daily tasks, Trust Protection Platform finds certificates that were not successfully checked for revocation within the last 24 hours. This can happen because the certificate does not have any CRL Distribution Points listed on the certificate. For example, LetsEncrypt certificates never use CRL distribution points. This could also happen because all listed CRL Distribution Points are either disabled or result in an error during check.

If a certificate was not successfully checked for revocation in the last 24 hours, Trust Protection Platform queries OCSP (Online Certificate Status Protocol) to check the revocation status of these certificates.

4. If a certificate matches, the certificate is marked as **Revoked**.

To view the revocation status of a single certificate

1. Open the **Certificate Inventory** and locate a certificate that you want to check.
2. Open the certificate's details page.
3. Click **Actions > Check Revocation**.
4. Look at the **Revocation Checking** section to see the status.
5. If the Results value is "Revocation check pending," refresh the page to see if the check has completed.

For information on viewing the revocation status of multiple certificates at the same time, see ["Viewing the revocation status of multiple certificates" on page 236](#).

Revocation and endpoint reason codes

When viewing the Result status in the **Revocation** area, you'll find one of several reasons displayed for the revocation of a certificate.

When a certificate is revoked, Trust Protection Platform displays the possible reasons why the certificate issuer did so. The issuer is responsible for specifying a reason. The reasons for revocation depend on whether the response came from the CRL or the OCSP.

CRL Revocation Response Codes

The CRL revocation response codes are defined in [Section 6.3.2\(b\) of RFC 5280](#) as outlined in the following table, which also includes a description of how certificates with these reason codes are treated by Trust Protection Platform.

Code Definition		Friendly Name	Description
0	unspecified	Unspecified	The reason was not given, or did not match an existing code. While it is possible to revoke a certificate with the <code>Unspecified</code> reason code, it is not recommended, as it does not provide an audit trail as to why a certificate is revoked. Indicates that the certificate was revoked for a reason not specified in the other codes. This option is not provided in TLS Protect, because it is not considered best practice to use it.
1	keyCompromise	Key Compromise	The token or disk location where the private key associated with the certificate has been compromised and is in the possession of an unauthorized individual. This can include the case where a laptop is stolen or a smart card is lost.
2	cACompromise	CA Compromise	The token or disk location where the CA's private key is stored has been compromised and is in the possession of

Code	Definition	Friendly Name	Description
			an unauthorized individual. When a CA's private key is revoked, this results in all certificates issued by the CA that are signed using the private key associated with the revoked certificate being considered revoked.
3	affiliationChanged	Affiliation Changed	The user's relationship with the organization has been terminated, indicated in the DN attribute of the certificate. This revocation code is most often used when an individual is terminated or has resigned from an organization. You do not have to revoke a certificate when a user changes departments, unless your security policy requires a different certificate be issued by a departmental CA. With this revocation code there is no cause to suspect that the private key has been compromised.
4	superseded	Superseded	A replacement certificate has been issued to a user, and the reason does not fall under the previous reasons. This revocation reason is most often used when a smart card fails, the password for a token is forgotten by a user, or the user's legal name has changed. There is no cause to suspect that the private key has been compromised.
5	cessationOfOperation	Cessation of Operation	Used anytime a certificate is no longer needed because the system or service that consumed the certificate is taken out of service before the expiration date on the certificate. If you select Original use no longer valid when you Revoke a certificate in TLS Protect, it will display this reason code, as this revocation reason was intended to express the idea of cessation of operation of a device or system, so the certificate should no longer be used or trusted.

Code Definition		Friendly Name	Description
6	certificateHold	Certificate Hold	A temporary revocation that indicates a CA will not vouch for a certificate at a specific point in time. Once a certificate is revoked with a <code>Certificate Hold</code> reason code, the certificate can then be revoked with another Reason Code, or it can technically be un-revoked and returned to use, though this is not supported by Trust Protection Platform. IMPORTANT Trust Protection Platform treats a <code>Certificate Hold</code> reason code as a permanent revocation. Even if the certificate is un-revoked by the CA, Trust Protection Platform will continue to treat the certificate as revoked. Therefore, do not apply a <code>Certificate Hold</code> to a certificate you intend to re-use in the future. Instead, revoke the certificate, and then issue a new certificate when you are ready to reapply it to the device.
7	{ value 7 is not used }	Reserved	This code is not used in the RFC, and does not appear anywhere in Trust Protection Platform.

Code	Definition	Friendly Name	Description
8	removeFromCRL	Remove from CRL	If a certificate is revoked with the <code>Certificate Hold</code> reason code, it is technically possible to "unrevoke" a certificate. The unrevoking process still lists the certificate in the CRL, but with the reason code set to <code>Remove From CRL</code>. Trust Protection Platform considers certificates marked with the <code>Remove from CRL</code> reason code as revoked. There is no way to tell the time period which the certificate was inactive, so for security best practice, these certificates are permanently revoked.
9	privilegeWithdrawn	Privilege Withdrawn	Indicates that a certificate (public key or attribute certificate) was revoked because a privilege contained within that certificate has been withdrawn. While a valid revocation code per the RFC, this revocation reason is not available in TLS Protect.
10	aACompromise	AA Compromise	Indicates that it is known or suspected that aspects of the AA validated in the attribute certificate have been compromised. You cannot select this as a revocation reason in TLS Protect because it is determined at a higher level.

NOTE Information for this table came was adapted from RFC 5280, Microsoft documentation ([https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc700843\(v=technet.10\)#revocation-reasons](https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc700843(v=technet.10)#revocation-reasons)) and the International Telecommunication Union (<https://www.itu.int/rec/T-REC-X.509-201210-S>).

The CA/Browser Forum (<https://www.cabforum.org>) issued the document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v. 1.2.5 (2015)". In chapter 13, it includes requirements for certificate revocation and status checking. Section 13.1.5 (page 22 of the linked PDF) specifies several situations in which a "CA shall revoke a Certificate within 24 hours".

OCSP Endpoint Response Codes

Code	Definition	Friendly Name	Description
0	successful	Successful	If the response is successful, the response will include a CertStatus value of one of the following: 0 - Good 1 - Revoked 2 - Unknown
1	malformedRequest	Illegal request	The request was not sent correctly to the OCSP. Verify your OCSP configuration.
2	internalError	Internal error in issuer	The OCSP responder replied with the code "Internal Error." This indicates that Trust Protection Platform was able to contact the OCSP endpoint, but an error occurred on their side. Try checking the certificate for revocation again, or wait for it to be checked by the CRL (if available for that certificate).
3	tryLater	Try again later	The OCSP endpoint was unable to process the request at this time. You should try the revocation check at a later time.
4	{ value 4 is not used }	Reserved	This value is not used in the RFC, and will therefore never appear in Trust Protection Platform.
5	sigRequired	Must sign the request	The OCSP endpoint requires that the request be signed before constructing a response. Trust Protection Platform does not support OCSP signature requests. Use another OCSP endpoint, or CRL.
6	unauthorized	Request unauthorized	The OCSP doesn't recognize this request as an authorized request. Either the client is not authorized to make the query, or the server is not capable of responding authoritatively. (See RFC 5019 Section 2.2.3.) Check your OCSP configuration or contact Venafi Support.

NOTE Information for this table was adapted from [RFC 6960 section 2.2](#) and [section 4.2.1](#).

If Trust Protection Platform detects an error with the OCSP response data, it may show one of the error messages in the following table.

Name	Description
None	An error occurred that isn't otherwise accounted for. Check the logs or call Venafi Customer Support for assistance.
Invalid Date	The OCSP response included an invalid date, so the data couldn't be verified.
Response Does Not Contain Certificate	The OCSP response does not contain the certificate status, so the status is unknown.
Signature Validation Failed	This means that the OCSP response, which is signed by the certificate authority, had an invalid signature, and therefore can't be trusted. In this case, contact your PKI administrator for what to do next. If you are the PKI administrator, you need to check your OCSP settings and make sure you are connecting to the correct OCSP endpoint.
General Error	This means that there was some other error during the parsing of the data or during communication with the OCSP endpoint. Check the logs for additional information about what happened, which should help you know how to resolve the issue.

Next Steps

Check the **General > Log** tab for useful details about actions taken on your certificate.

Disabling (or enabling) CDP monitoring and revocation checking

By default, Trust Protection Platform's revocation monitoring feature is enabled. But you can disable and re-enable the feature. You can disable revocation checking, though this is not a recommended practice.

Certificates that are **Expired**, **Disabled**, **Revoked**, or marked **Certificate Hold** are no longer checked for revocation.

You can only turn off Revocation checking and CDP monitoring for the whole platform by disabling the Certificate Revocation Service Module for all engines in each engine's Venafi Configuration Console. This turns off BOTH Revocation checking and CDP monitoring. You can't disable or enable one without the other.

To disable (or enable) Revocation monitoring and CDP monitoring

1. On each engine, open the Venafi Configuration Console.
2. Click the **Product** node.
3. Locate the **Certificate Revocation Monitoring** component.
4. In the **Actions** panel, click **Disable** (or **Enable**).
5. [Conditional] If you are *disabling* the component, you need to repeat for every engine. If you are *enabling* the component, you should only enable it on engines that have access to the CDP and OCSP endpoints.

Viewing the revocation status of multiple certificates

Although not included by default, you can add the Revocation Status column to the View tab in order to load and see the revocation status of all certificates.

To add the Revocation Status column to the certificate inventory

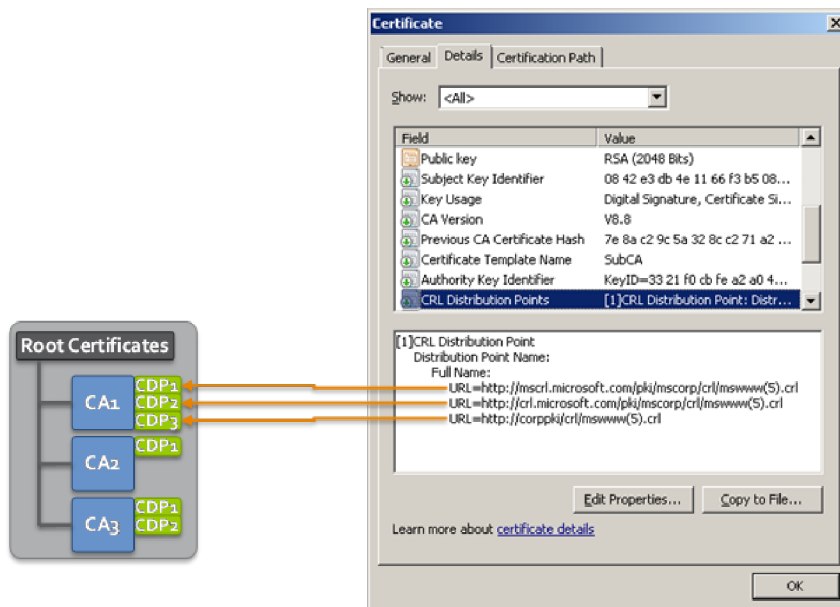
1. In the Aperture menu, click **Inventory > Certificates**.
2. Click **Edit Columns**.
3. In the **Search** box, type:
4. Use the arrows to move the column to the position you want.
5. Click **Apply**.

Validating Certificate Revocation Lists - Overview

Ensuring your certificate validation statuses match the status of the certificate on the CA is important. If a CRL expires or is unavailable, it can cause multiple system outages for all systems with certificates that rely on that CRL Distribution Point (CDP) for verification. Trust Protection Platform checks the CDPs on a scheduled basis to verify that the endpoint is active. If a CDP goes down, you need to take immediate action to prevent outages. The Trust Protection Platform Certificate Revocation List (CRL) Verification Service verifies CRLs to ensure that they are valid and available for revocation checking. If a CRL is within a configurable time-period prior to expiration, the service sends a notification to one or more administrators so that they can ensure it is updated.

The CRL Verification Service checks CRLs on each CDP on which they are located. To accomplish this, the CDP location information for each verified CRL is configured in Trust Protection Platform on CA certificates in the Policy Tree Roots tree. CDP information is added to Trust Protection Platform in three ways:

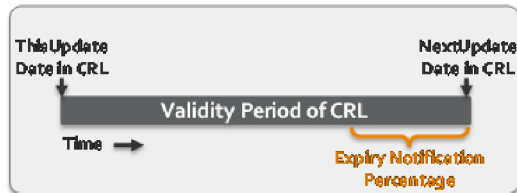
- **Automatic population:** Trust Protection Platform scans certificates in the inventory, and searches for information about the certificate's issuer. If the CDP for a certificate is not already in the Policy Tree Roots tree, it is added. For more information see ["Validating Certificate Revocation Lists - Overview" on the previous page](#).
- **New CA Certificate:** When a CA certificate is added to the Roots tree, Trust Protection Platform checks the certificates in the Policy tree that have been issued by that CA and adds any discovered CDPs to the CA certificate object.
- **Manually:** CDP entries can be added to an individual CA certificate object by entering the CDP location information (the URL to the CDP).
- **Revocation checking:** Trust Protection Platform checks for revoked certificates on a scheduled basis, automatically. To learn more about how revocation checking works, see ["Checking the revocation status of certificates" on page 228](#).



The time-frame prior to the NextUpdate date when the CRL Verification Service will send notification warning of expiration is configurable using the Expiry Notification Percentage. The Expiry Notification

Percentage is a percentage of the CRL validity period (Published Date to NextUpdate) and is used to determine how long before CRL expiration that the CRL Verification Service should send expiration warning notifications.

NOTE The *Next Update* attribute is functionally the expiration date of the CRL. Thus, you can extrapolate the validity period of the CRL by subtracting the *Published Date* from the *Next Update*.



This percentage is set at the root of the Roots tree (to apply to all CA certificates) or on individual CA certificates (overriding the value set at the root). Each time that the CRL Verification service runs, it connects to each CDP, retrieves the CRL, and calculates the amount of time until the NextUpdate date. If that time is less than the Expiry Notification Percentage, a notification is sent.

About Supported URL Formats

Trust Protection Platform CRL Verification service supports the following URL formats for CDPs:

- HTTP (e.g. `HTTP://crl.venafi.com/enterprise.crl`)
- FILE (e.g. `FILE://crl.venafi.com/CertEnroll/QA-CA.crl`); format requires `FILE:` followed by any valid Windows path.

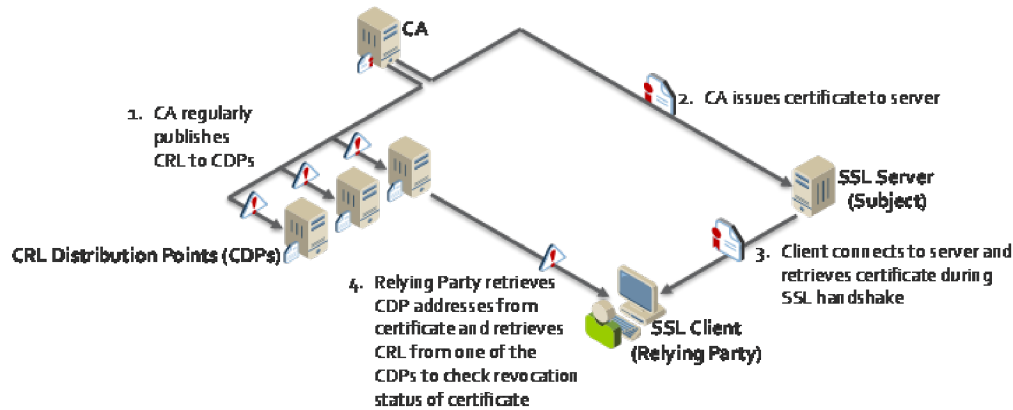
Trust Protection Platform expects all endpoints to be configured for anonymous authentication. When Trust Protection Platform is installed on a Windows server that is joined to a domain, Trust Protection Platform leverages the permissions of the account that VPlatform is running under if a FILE endpoint requires authentication.

Understanding CRLs and CDPs

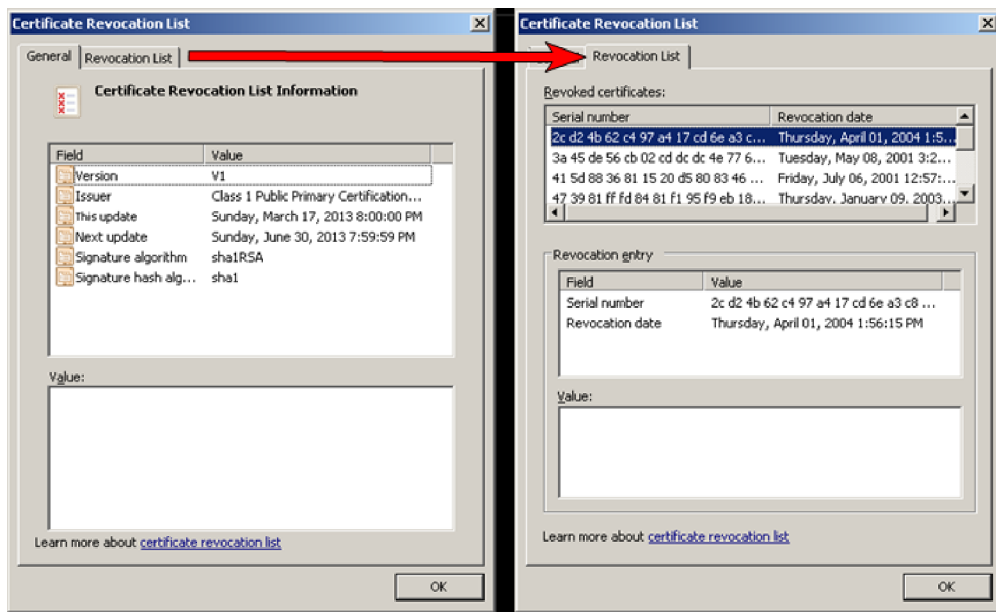
Before discussing CRLs and CDPs, it is helpful to distinguish two roles: the Subject and the Relying Party.

A Subject is a person or system to which a certificate is issued. A Relying Party is the person and/or system that uses a Subject's certificate for secure communications or verifying digital signatures. For example, a web server to which an SSL certificate is issued is a Subject and the Relying Party is an user connecting to the web server with a browser.

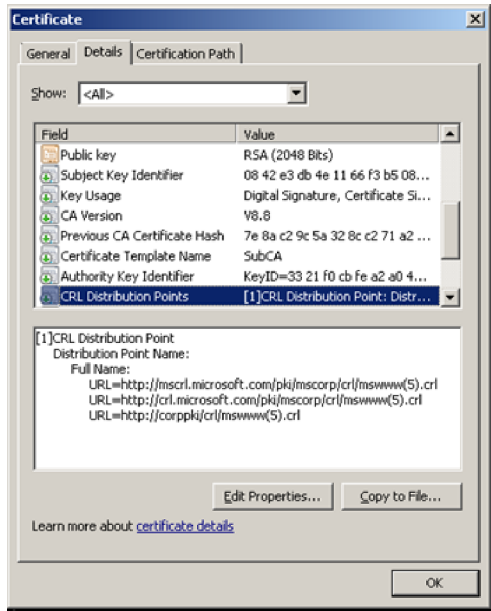
A certificate authority (CA) revokes a certificate when it is no longer trustworthy, such as when a Subject is misidentified in a certificate or the Subject's private key is compromised. CAs publish certificate revocation lists (CRLs) so Relying Parties know which certificates have been revoked.



CRLs include a list of certificates a CA has revoked as well as other information. CRLs should include two dates: the date on which the CRL was last updated (Published Date) and the date on which the CRL will be updated next (NextUpdate). The period of time between these two dates is the validity period of the CRL. CAs should update the CRL on all CDPs on or before the date specified in the NextUpdate field of a CRL. If a Relying Party retrieves a CRL with a `NextUpdate` date that has passed, the Relying Party should not continue. This can result in downtime if the Relying Party is an automated system. Therefore, it is critical that CRLs be kept up-to-date. The following image shows a sample CRL.



CAs publish CRLs in one or more locations, called CRL Distribution Points (CDPs), where they can be easily accessed by Relying Parties. The CA places the address(es) of CDP(s) for its CRL in each certificate it issues so that Relying Parties know their locations. The following figure shows a sample certificate that contains three CDP locations in the CDP extension.



Certificate Distribution Point Monitoring in Trust Protection Platform

CRLs are digitally signed by the CA, which is how you validate their authenticity, since you use an insecure connection to retrieve them (for example, HTTP; you should not use HTTPS). If a CDP goes down, it can result in a multi-system outage for all certificates that check revocation status (including the Venafi Agent). The CDP checking functionality in Trust Protection Platform scales well for systems of all sizes, such that frequent checks (including hourly checks) don't have a negative impact on system performance.

The CDP checking functionality also updates the revocation status of any affected certificates each time the CRL is loaded.

Trust Protection Platform's custom endpoints functionality allows you to use a load balancer for high availability monitoring, while still allowing Trust Protection Platform to connect to every endpoint covered by the load balancer to ensure all your systems are working properly.

Enabling CRL Verification

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.

On a new installation, by default, the CRL Verification Service is enabled to verify the status of Certificate Revocation Lists (CRLs). Trust Protection Platform verifies CRLs on a configurable basis (at least every 24 hours). It is possible to enable the CRL Verification Service for all engines or on individual Trust Protection Platform engines.

You can also enable or disable individual CRL Distribution Points (CDPs). All CDPs are enabled by default when they are added automatically.

NOTE It is not recommended to use the HTTPS protocol to update your CDPs. CDP servers are typically configured to use HTTP. If a CRL retrieval fails, verify that you are using HTTP.

CDP Status Result Options

When the CRL Verification checks the CDP, the following statuses are possible results.

- Success
- Not supported
- Unable to retrieve the data using the end point: {error}
- Unable to parse the data node: {error}
- The Delta CRL is specified for an older CRL than the one currently being used.

- The CRL is newer than the Delta CRL is specifying.
- Expired on {date}
- Expires on {date}

The status is shown on the **CRL Distribution Points** list, in the **Status** column.

Enabled/Disabled	URI	Status	Description	Last Verification	Last Successful Ve...	Publish Date	Expires On
Enabled	http://crl.certigna.fr/certigna.crl	Success		6/18/2019 2:19:27...	6/18/2019 2:19:27...	5/29/2019 5:14:51...	5/28/2020
Enabled	http://crl.dhimyotis.com/certigna.crl	Success		6/18/2019 2:19:27...	6/18/2019 2:19:27...	5/29/2019 5:14:51...	5/28/2020

At any point, you can click the **Verify Now** to immediately validate the highlighted CRL Distribution Point.

NOTE When you click **Verify Now**, the validation check happens immediately, and the next scheduled check will be skipped for performance reasons. The normal schedule will resume at the next check interval.

The status is also shown as part of the **Revocation Result** on the **Certificate Summary** tab when you select a certificate in the Policy tree.

Certificate Status	
OK	
Expiration Date	8/15/2019 10:22:25 AM
Revocation	Last Check: 6/18/2019 2:19:31 AM Result: Revocation check via CRL, CRL status: Success
Lifecycle Stage	none
Validation	Last Check Status

NOTE This only validates the single row that is highlighted. If you wish to verify all endpoints listed in the table, you will need to verify them one-by-one.

To Modify CRL Verification for all engines

1. From the **Tree** menu, select **Platforms**.
2. Select the root of the **Platforms** tree.
3. Click the **Certificate Revocation** tab.
4. Under **Settings**, click the **Check in Interval (times daily)** drop-down list and select the number of times you want to perform CRL verification.

Value	Additional Information
1	Check once per day at 12:00 AM (based on the time zone set for the engine that is assigned to perform the work).
2	Check twice per day 12-hour intervals.
3	Check three times per day 8-hour intervals.
4	Check four times per day at 6-hour intervals.
6	Check six times per day at 4-hour intervals.
8	Check eight times per day at 3-hour intervals.
12	Check twelve times per day at 2-hour intervals.
24	Check every hour.

NOTE For all intervals except daily, the time interval begins when Trust Protection Platform services are enabled on that engine. Thus, checking begins for an engine when you restart services. There are controls in place to ensure a certificate's revocation status isn't checked too frequently. If a certificate's revocation status has been checked recently, the next scheduled revocation check will be skipped.

To Disable CRL Verification on a particular engine

1. From the **Platform menu bar**, click **Policy Tree**.
2. Select the **Platforms** tree.
3. Select the engine on which you want to enable CRL Verification.
4. Select the **Certificate Revocation** module in the tree below the engine.
5. Click the **Settings** tab.
6. Under **Disable this module**, select the **Disable this module** check box, and then click **Save**.

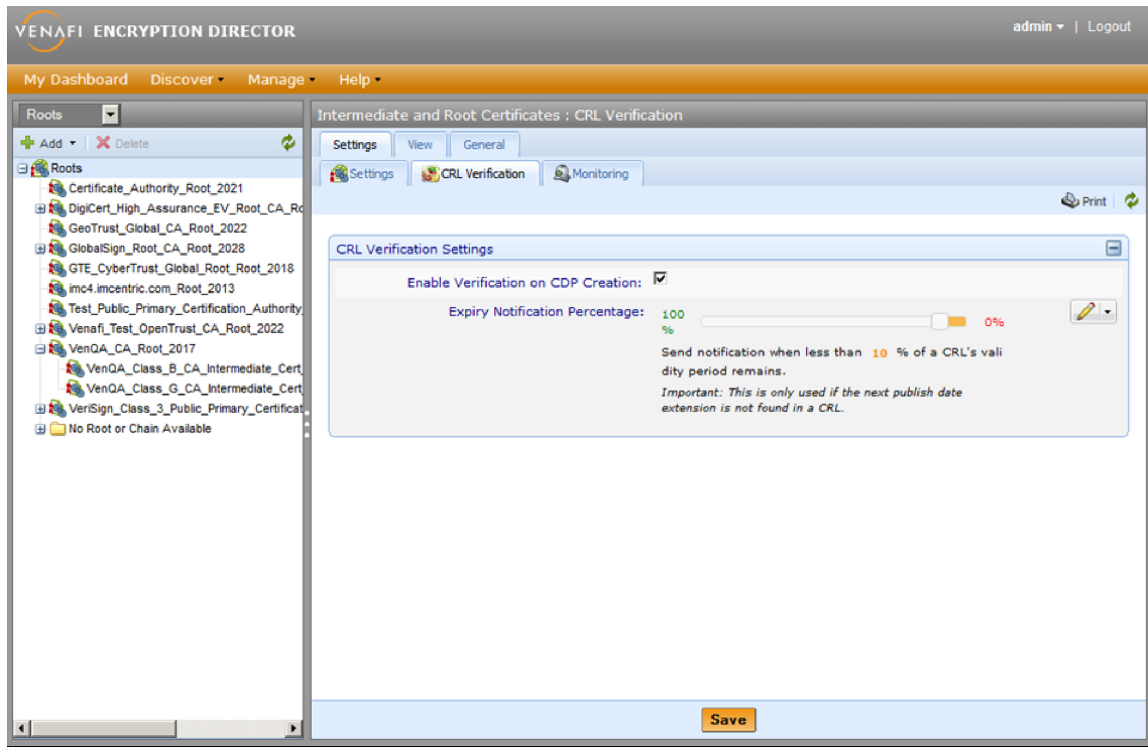
To enable CRL Verification on a CDP Entry

1. Select the **Roots** tree.
2. Select the CA certificate.
3. Select the **CRL Verification > CRL Distribution Points** tab.
4. Click on the CDP entry that you want to enable or disable.
5. Click **Edit**.
6. Select or clear the **Disable Verification** checkbox.

To Modify CRL Verification Expiration Notification Percentage

You can modify when you want to be notified if a CRL is about to expire. This setting is based on the percentage of time before a CRL expires because different CRLs will have different validity periods. By setting the notification percentage, you don't have to worry about knowing a specific CRL's validity period before you can select an appropriate expiration notification percentage.

1. Select the **Roots** tree.
2. Select the **Settings > CRL Verification** tab.

3. Choose the **Expiry Notification Percentage**.

Adding CDP Entries

Certificate revocation list (CRL) Distribution Points (CDPs) for Trust Protection Platform-verified CRLs are stored on CA certificate objects in the Roots tree. The CA certificate in the Roots tree to which a CDP entry is added corresponds to the CA that issues the CRL and publishes it to the CDP.

CDP entries are added in one of three ways:

- **During Install:** When Trust Protection Platform is initially installed or when an older version of Trust Protection Platform is upgraded to a version that includes CRL Verification, Trust Protection Platform will then evaluate all of the certificates in the Policy and Root trees for CDP information. If the CA certificate corresponding to the CA that issued each certificate is in the Roots tree, the discovered CDP information is added to the CA certificate object.
- **Addition of New CA Certificates:** When a CA's certificate is added to the Roots tree, Trust Protection Platform checks the certificates in the Policy tree that have been issued by that CA and adds any CDPs within those certificates to the CA certificate object.

NOTE Adding a new certificate to the certificate inventory with data in the `CA Issuer` attribute will cause Trust Protection Platform to automatically add the certificate chain to the Roots tree. Since the signature revocation lists and OCSP responses are verified by Trust Protection Platform, the root certificates must exist in the roots tree to properly verify responses.

- **Manually:** You can add CDP entries manually by entering the CDP location information (the URL to the CDP) on a CA certificate object. Generally, you add a CDP entry manually if certificates issued by a CA do not show all CDP locations.

Manually adding a CDP entry

1. From the **Platform menu bar**, click **Policy Tree**.
2. From the **Roots** menu, select the certificate to which you want to add a CDP entry.
This is the certificate for the CA that publishes the CRL to the CDP being added.
3. Click the **CRL Verification** tab.
4. Click **Add**.
5. In the pop-up window, enter the information for the custom CRL Distribution Point.
 - **Disable Verification.** Check to disable CRL verification for this CDP.
 - **URI.** Enter the URL for the CDP.
 - **Description.** (Optional) Enter a description providing additional information about this CRL endpoint.
6. Click **OK**.

After clicking **OK**, the CDP you have entered is then scheduled for processing by a Trust Protection Platform engine.

About Supported URL Formats

Trust Protection Platform CRL Verification service supports the following URL formats for CDPs:

- **HTTP** (e.g. `HTTP://crl.venafi.com/enterprise.crl`)
- **FILE** (e.g. `FILE://crl.venafi.com/CertEnroll/QA-CA.crl`); format requires `FILE:` followed by any valid Windows path.

Trust Protection Platform expects all endpoints to be configured for anonymous authentication. When Trust Protection Platform is installed on a Windows server that is joined to a domain, Trust Protection Platform leverages the permissions of the account that VPlatform is running under if a FILE endpoint requires authentication.

Setting the Expiry Notification Percentage

Certificate revocation lists (CRLs) should be updated by certificate authorities (CAs) prior to the NextUpdate date. It is recommended to configure your CA to publish your CRL updates well before the expiration of the previous CRL. That way, if there is a failure, you have time to update it or fix it before certificates relying on it can't be validated. If the CRL is not updated at this time due to a communications (or another) failure, then there is the risk that the CRL will expire while online and result in system outages.

The Trust Protection Platform CRL Verification Service can be leveraged to regularly check CRLs and will send expiration warning notifications at a specified time prior to CRL expiration to prevent system outages. The amount of time prior to expiration that notifications are sent is calculated using the Expiry Notification Percentage, which is a percentage of the CRL validity period.

EXAMPLE Suppose that Trust Protection Platform retrieves a CRL with a *Publish Datedate* of September 10, 2015 and *Next Update* of Sept. 20, 2015. The Expiry Notification Percentage is set to 20%; therefore, notifications will start being sent 2 days prior to expiration (20% of the 10-day validity period).

Using a percentage (rather than a specific number of days) lets you specify a default value for all CRLs. In addition, Trust Protection Platform sends automated notifications about pending expirations based on the length of each CRL's validity period.

To set the default Expiry Notification Percentage

1. From the **Platform menu bar**, click **Policy Tree**.
2. Select the **Roots** tree.
3. Select the **Root Certificates** node in the tree.
4. Click the **Settings** tab.
5. Set the **Expiry Notification Percentage**, and then click **Apply**.

NOTE You can lock this value so that it cannot be changed on subordinate certificate objects by selecting the policy icon to the permission of the setting and clicking **Lock This Value**.

To set the Expiry Notification Percentage for a single CRL

1. Select the **Roots** tree.
2. Select the CA certificate that you want to modify.
3. Click the **Certificate > Settings** tab.
4. Set the **Expiry Notification Percentage**, and then click **Apply**.

Disable a CDP entry or modify a CDP description

You can modify some properties of a single CDP entry by selecting a CDP item from the CRL Verification tab.

To edit a single CDP entry

1. From the **Platform menu bar**, click **Policy Tree**.
2. From the **Roots** menu, select the CA certificate that you want to modify.
3. Select the **CRL Verification** tab.
4. Select the CDP entry to edit.
5. Click **Edit**.
6. Edit the desired settings.

NOTE You cannot change the URL of the CDP, even if it is a custom-created CDP. If you want to change the URL, you need to create a new CDP entry.

TIP You cannot delete a CDP whose source is from a certificate. You can only delete custom CDPs. However, all CDPs, regardless of source, can be disabled.

Configuring CRL notifications and email messages

By default, the Trust Protection Platform CRL Verification Service sends notifications when CRLs are about to expire or have expired. It is possible to change the settings for these notifications or send notifications for other events, such as if the CRL is not correctly signed or cannot be located.

There are two notification rule templates installed by default in VCC in the Logging node, Logging\Notification Rules\Templates when the CRL Verification Service is installed: **CRL Nearing Expiration** and **Expired CRL**. You can disable these rules if you would not like to receive notifications.

The email notifications that are triggered by these rules are configured in VCC on the Logging node. Logging\Channels\Templates folder. The default notification templates are: **Email to Owner - CRL Expired** and **Email to Owner - CRL Near Expiration**.

You can also create new rules.

Pushing Certificates and Private Keys to Applications

Trust Protection Platform can install, or “push,” certificates and private keys to applications associated with Certificate objects. If the certificate and private key already exist on the target server, the push operation replaces the existing certificate and private key.

IMPORTANT The Application object associated with the certificate must be correctly configured for Trust Protection Platform to authenticate with the target application and copy the certificate and private key file(s) to the correct Directory in the application's local file system.

The Push feature provides an easy and convenient way to install new certificates or update existing certificates on managed applications. However, 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
- You can associate certificates with applications from either the Certificate or Application object configurations.

The following sections review the procedures and requirements to associate certificates with applications:

This chapter contains the following topics:

Pushing a certificate and private key to an application

You can push an application object's associated certificate and private key to the application using Push  button.

NOTE To push a certificate and private key to an application, you must have the *Write* permission to the application object and either *Write* or both *Associate* and *Read* permissions to the certificate object.

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
- You have the correct permissions to the application object and the associated certificate object
- You must have Write permissions to the current Application object

IMPORTANT If the certificate and private key already exist on the target server, the push operation replaces the existing certificate and private key.

To push a certificate or private key to an application from the Application object

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. In the **Policy** tree, select the Application object to which you are going to push the certificate and private key.
3. On the application object's **Settings** tab, click **Push** .

The application object associated with the certificate must be correctly configured to enable Trust Protection Platform to provision the certificate to the application.

Pushing a Certificate and Private Key to an Application from the Certificate Object

You must have the *Private Key Read* or *Write* permissions to the Certificate object and either *Write* or both *Associate* and *Read* permissions to the Application object to push a certificate and private key to an application.

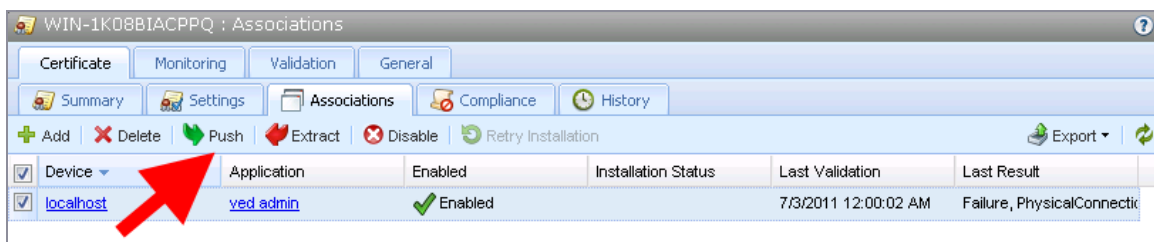
Trust Protection Platform notifies you that the application has been queued for a certificate and private key push operation.

If an error occurs during the push operation, the object goes into an error state and the operation does not continue until an administrator takes action. Both the Certificate and Application reflect the error.

IMPORTANT The Application object associated with the certificate must be correctly configured for Trust Protection Platform to authenticate with the target application and copy the certificate and private key file(s) to the correct Directory in the application's local file system.

To push a certificate and private key to an application from the Certificate object

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. In the Policy tree, select the Certificate object from which you are going to push the certificate and private key.
3. Click the **Certificate > Associations** tab.



4. Select the Application where you want to push the certificate and private key.
5. Click **Push** .

ACME integration with TLS Protect

Automatic Certificate Management Environment, usually referred to as ACME, is a simple client/server protocol based on HTTP. The client represents the applicant for a certificate (e.g., a web server operator), and the server (Trust Protection Platform) represents the CA. ACME enables TLS Protect to verify that the applicant owns some number of domains, and then enables the applicant to request certificates for those domains.

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.

To learn more about *certbot*, visit <https://datatracker.ietf.org/wg/acme/about/>.

To learn more about *win-acme*, visit <https://www.win-acme.com/manual/getting-started>.

To learn more about *acme.sh*, visit <https://github.com/acmesh-official/acme.sh>.

About the ACME protocol

The Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating interactions between certificate authorities and their users' web servers, allowing the automated deployment of public key infrastructure at very low cost. It was designed by the Internet Security Research Group (ISRG).

Venafi Trust Protection Platform supports some features from both the ACME v1 and v2 protocols.

ACME v1 supports issuing certificates for fully-qualified domains, but does not support issuing wildcard certificates.

ACME v2 is not backwards-compatible with ACME v1. The version 2 *specification* details support for wildcard domains, allowing for multiple subdomains to be covered by a single TLS certificate (support for this feature is slated for a future Venafi Platform release).

To learn more, visit <https://letsencrypt.org/docs/acme-protocol-updates/> and https://en.wikipedia.org/wiki/Automated_Certificate_Management_Environment.

About Venafi Support for ACME v2

In this release of Venafi Platform, we support the following:

- `http-01` and `dns-01` challenges
- DNS TXT verification of domain control
- Wildcard certificate issuance
- All required (MUST / REQUIRED / SHALL) components of the ACME v2 specification ([RFC8555](#))

- Certificate enrollment with multiple domains
- Elliptic curve key algorithm for account or certificate
- Account deactivation
- Certificate revocation through ACME.

This release *does not* support:

- KeyChange endpoint

About using the win-acme client

A windows-native ACMEv2 client that is supported by TLS Protect is win-acme, which is a client that is simple, making it easy to start with, but it is also powerful enough for almost any use case. Learn more about it at <https://www.win-acme.com>.

You can use the win-acme client, but please be aware of the following limitations:

- Your Venafi server cluster must use a supported Windows operating system. For win-acme, you must be using Windows Server 2016 or later.
- FIPS compliance should NOT be enabled on the Venafi server.
- In the win-acme settings JSON file, the `DefaultBaseUri` field should be set to the TLS Protect ACME server using this pattern:
`https://<server_url>/vacme/v2/<tpg_sub_folder>/`
- The win-acme client only supports revocation for the reason `Unspecified`.
- The win-acme client sends revocation requests to TLS Protect using the account key.

About using the acme.sh client

Acme.sh is a fully compliant ACME v2 client that supports ECDSA and wildcard certs, making it a powerful tool for managing certificates. See github.com/acmesh-official/acme.sh.

Acme.sh supports both HTTP-01 and DNS-01 validation types. Here are examples from how to use them:

```
# Issue a certificate using HTTP-01 validation
acme.sh --issue --webroot /var/www/html/ -d www.test.org
```

```
# Issue a certificate using DNS-01 validation
acme.sh --issue --dns dns_nsupdate --dnssleep 3 -d *.test.org
```

For the most accurate and current information, see the official documentation at github.com/acmesh-official/acme.sh.

Installing the ACME Service

Before you can use the ACME service, you must install and enable it on your Trust Protection Platform server. If the ACME Service was not installed during installation of Trust Protection Platform, you can add it using the Venafi Configuration Console.

To add the ACME component after Trust Protection Platform has already been installed

1. From the Windows Start menu, click **Venafi Configuration Console (VCC)**.
2. Click the **Product** node.
3. In the **Product Components** panel, under the **Certificate Manager** (or **Mobile Certificate Manager**) section, click **ACME Service**.
4. In the **Actions** panel, click **Enable**.

Enabling and configuring ACME using TLS Protect

You can enable and configure the ACME service using TLS Protect.

NOTE Before you do this, make sure that the ACME server component is installed. See "Installing the ACME Service" above.

To enable and configure ACME

1. From the **TLS Protect menu bar**, click **Configuration> ACME**.
2. You will be prompted to **Enable ACME?**. Click **Yes**.

3. Under **Create Certificates in**, select the folder into which ACME Service certificates will be placed.

IMPORTANT A CA template must be assigned to the folder that you select. See [Assigning a CA template to a policy folder](#).

Also, make sure user accounts have Create and Write permissions to the new sub-folders where certificates will be created and stored. If permissions are not correctly set and the user tries to create a certificate in the folder, an error message saying `ACME - Insufficient Permissions` is written to the log file.

4. (Optional) Select **Automatically create folders if they don't exist**.
 - When selected, if a folder doesn't exist when the certificate's location is specified, a folder with that name will be created. In the certbot request's URL, the new folder's name cannot contain uppercase letters.
 - When cleared, certificate requests will fail if the folder doesn't already exist. An error message will be sent via certbot and an event will be logged in Trust Protection Platform. Certbot will display a similar message in the letsencrypt.log file.
5. Match new ACME certificate requests to existing certificate objects. (Enabled by default for new installations)
 - When selected, new ACME certificate requests will be matched via the SAN(s) and placed as the active certificate in the matched certificate object. The active certificate is then placed in the previous versions / history tab of the certificate object. This also changes the certificate object naming pattern for the new certificate object so it no longer contains a unique time stamp but contains only the first domain from the request. Matching will be applied only if the renewal request comes from the same account that requested the initial certificate; otherwise, a new certificate object will be created.

- When cleared, new ACME certificate requests will create new certificate objects without matching to existing certificate objects. The certificate objects naming pattern will contain the first domain from the request and a unique time stamp.
- For these settings to take effect, Internet Information Server (IIS) must be reset.

NOTE Renewals may incur additional charges. If the Certificate Authority supports re-issuance, the renewal requests may be handled as a re-issuance or as a replacement. This can lead to the Certificate Authority revoking the historical certificate.

6. Type the ACME URL Hostname.

NOTE The default name is the fully qualified domain name (FQDN) of the engine. You have the option to change it here.

7. When you're done, click **Save**.

To verify server configuration

In a web browser, type `https://[ACME_server_FQDN]/vacme/[v1|v2]/[TPP_folder]/directory`

For example:

`https://tpp-alpha.venafi.com/example/vacme/v1/test/directory`

The displayed text confirms that the ACME server is working. You can also see the URLs that the ACME client will use (internally) to register and request certificates.



To change an engine's default URL Hostname

1. In Policy Tree, go to the **Platforms** tree.
2. In **Platforms**, click an Engine name.
3. Under **Trust Protection Platform URL HostNames**, in the **Automatic Certificate Management Environment (/VACME)** field, enter the hostname of the ACME server.

NOTE The default name is the fully qualified domain name (FQDN) of the engine.

BA2012AUTO : Settings

Network Device Enrollment Venafi Trust Protection Platform General Support

Settings Proxy

Print

Settings

Run daily tasks at: 12:00 AM

Check for work every: 15 seconds

Operations

Certificate: \\VED\\Policy\\Venafi Operational Certificates\\BA2012AUTO

Logging

Log Debug: ☐

Discovery Zones

Discovery Zones:

Add Edit Remove

Trust Protection Platform URL HostNames

Automatic Certificate Management Environment (/VACME):

Aperture (/Aperture):

Client Subsystem for Agents (/VEDClient):

Network Device Enrollment (/VEDSCEP):

REST API (/VEDSDK):

User Portal (/Portal):

Web Administration Console (/VEDAdmin):

4. Click **Save**.

ACME domain challenge

ACME v1

Trust Protection Platform supports HTTP domain validation methods for verifying that the user has authorized access to the requested domains. This means that Trust Protection Platform will generate a challenge and return it to the ACME client user and subsequently verify the challenge using HTTP (http-01)

as indicated by the user in the request.

If a requested certificate has a Common Name (or DNS SAN) of *www.vfidev.com*, the HTTP domain validation would consist of an HTTP GET request for *http://www.vfidev.com/.well-known/acme-challenge/<acme token>* and is expected to return HTTP 200 OK *<acme key authorization value>* where the *<acme token>* and *<acme key authorization value>* are the challenges our ACME server sent back to the requesting ACME client (e.g. certbot).

See <https://tools.ietf.org/html/draft-ietf-acme-acme-06#section-8.2> for more information.

- In order for HTTP validation to be successful, the domain of the certificate request must match the domain to which the web server resolves.
- A certificate is only issued if HTTP validation is successful for at least one of the domains specified in the request. If any domains fail validation, the ACME server will respond with an error and those domains are excluded from the certificate that is issued.

ACME v2

Trust Protection Platform conforms to the ACME v2 specification domain challenge requirements, for HTTP (http-01) as specified in [section 8.3 of the specification](#) or through DNS (dns-01) as specified in [section 8.4 of the specification](#).

- Trust Protection Platform should be able to resolve the DNS server to confirm the challenge and vice versa.
- TXT record should be in format: `_acme-challenge.domain` according to <https://datatracker.ietf.org/doc/html/rfc8555#section-8.4>.

About requesting an ACME certificate using certbot

You can easily request and enroll a certificate using certbot and your ACME server.

TIP For a list of basic certbot commands for use when working with users, registrations, and certificates see "Basic ACME certbot commands" on the facing page.

The following example shows:

- The certbot command for requesting a certificate with two domains (*chicago-cubs.venafi.example* and *cubs.venafi.example*) from the ACME server to an Apache server.

- That *webroot* is a feature of certbot that automates the HTTP domain validation (putting the ACME challenge on the web server so that Trust Protection Platform can check it).
- That certbot also supports a manual mode in which the user must copy and paste the ACME challenge to a file and put it on his or her web server manually.

```
certbot certonly --webroot \  
--server https://tpp.venafi.example/vacme/v2/chicago/directory \  
--cert-name cubs \  
-d chicago-cubs.venafi.example -d cubs.venafi.example \  
--webroot-path /var/www/html
```

When the certificate request is successful, you will receive a note that includes details about the new certificate.

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/cubs/fullchain.pem. Your cert will expire on 2017-06-30. To obtain a new or tweaked version of this certificate in the future, simply run certbot again. To non-interactively renew **all** of your certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>
Donating to EFF: <https://eff.org/donate-le>

Subject: CN=chicago-cubs.venafi.example
DNS:chicago-cubs.venafi.example, DNS:cubs.venafi.example

Basic ACME certbot commands

Here are a few basic commands to use when working with certbot and Trust Protection Platform's ACME implementation.

Request a certificate and place it in the specified folder:

```
certbot certonly --server https://[ACME_server_FQDN]/vacme/v2/[tpp_sub_folder]/directory
```

IMPORTANT The `[tpp_sub_folder]` variable must be expressed in lower-case letters, regardless of the capitalization in Venafi Platform.

Also, make sure user accounts have Create and Write permissions to the `[tpp_sub_folder]` where certificates will be created and stored. If permissions are not correctly set and the user tries to create a certificate in the folder, an error message saying `ACME - Insufficient Permissions` is written to the log file.

Example URL: `https://platform.venafi.example/vacme/v2/chicago/directory`

- If your user hasn't been registered, then the `certonly` command will register while also requesting a certificate.

Register your user with the Venafi ACME server:

```
certbot register --server https://[ACME_server_FQDN]/vacme/v2/[tpp_sub_folder]/directory -m [User_Email_Address]
```

Example URL: `https://platform.venafi.example/vacme/v2/chicago/directory`

Request a certificate and specify the name and SANs:

```
certbot certonly --server https://[ACME_server_FQDN]/vacme/v2/[tpp_sub_folder]/directory --cert-name example.com -d example.org -d test.example.org
```

Troubleshooting

Delete the certificate that certbot created locally: `rm -f -r /etc/letsencrypt/live/[<certificate name>]`

Delete the renewal configuration for a certificate that certbot enrolled: `rm /etc/letsencrypt/renewal/[certificate conf]>`

- `rm /etc/letsencrypt/renewal/<certificate.conf>`

Remove an ACME registration from certbot: `rm -r /etc/letsencrypt/accounts/[TPP server FQDN]/vacme/directory/[tpp_sub_folder]tpphstdir`

NOTE Consider the following key points:

- E-mail addresses are tied to local, Active Directory, or LDAP identities when registering with ACME. If Trust Protection Platform is unable to locate your user account by e-mail address, your registration will fail.
- Make sure user accounts have Create and Write permissions to the `[tpp_sub_folder]` where certificates will be created and stored. If permissions are not correctly set and the user tries to create a certificate in the folder, an error message saying `ACME - Insufficient Permissions` is written to the log file.
- The ACME server URL for registration and certificate requests **must** be expressed in lower case letters.
- Active Directory group e-mails may also be used to register with the ACME server. However, you won't be able to view account and activity details for Distribution Groups.

If you need to use a Distribution Group, contact Customer Support (support@venafi.com) for help.
- The root certificate that issued the certificate securing Trust Protection Platform's ACME server URL needs to be added to certbot's trust store. This means that your Trust Protection Platform server needs a signed certificate.

ACME v2 revoke certificate endpoint

You can easily revoke a certificate using certbot and your ACME server.

TIP For a list of basic certbot commands for use when working with users, registrations, and certificates see ["Basic ACME certbot commands"](#) on page 259.

The endpoint supports:

- A request signed with the key of the identity that issued the certificate whose identity is valid (present in the identity provider)
- A request signed with the key of the certificate itself

When the endpoint receives a request, a revocation request is sent to the CA.

If the revocation request is rejected by the CA, the response is passed to the ACME client along with a revocation code number (if provided by the CA), and Venafi Platform will show the certificate as "in error."

If the revocation request is approved by the CA, the response is passed to the ACME client, and is marked as Revoked in Venafi Platform, and processing for that certificate is disabled.

You can use the revoke endpoint to revoke a certificate in the following ways:

Method	Code Sample
Using the account key	<pre>certbot revoke --server https://[ACME_server_FQDN]/vacme/v2/ [tpp_sub_folder]/directory --cert-name {cert-name}</pre>
Using the certificate private key	<pre>certbot revoke --server https://[ACME_server_FQDN]/vacme/v2/ [tpp_sub_folder]/directory --cert-path {cert-path} --key-path {key-path}</pre>

Viewing ACME certificates

ACME certificates can be viewed based on Identity. Identity is tied to the email address that was used to register the account.

To view ACME certificates

1. In Aperture, click **Inventory > Identities**.
2. Use filters to find the Identity you want.
3. Click the Identity name.
4. In the side bar, click **ACME**.

A list of registrations for that Identity is displayed along with the corresponding Public Key Fingerprint, Domains, and Certificates.

Domains represents the total number of unique names (Common Names and DNS SANs) that were requested by the ACME account, along with the number of those that were successfully validated and appear in issued certificates.

5. Click the number under **Certificates** to see a detailed list.

DashboardsInventoryDiscoveryAgentsReportsConfiguration

Search

Helpadmin

localadmin

Overview

Certificates

Mobile Agents

ACME

4 Accounts

	Registered On	Public Key Fingerprint	Domains	Certificates
☐	12/3/2016 7:07 PM	aafdasklfasdopuqwerpouadflouooykgdt:ajsfdhkjpustf	3 (2 Valid)	1
☐	12/3/2016 7:07 PM	aafdasklfasdopuqwerpouadflouooykgdt:ajsfdhkjpustf	3 (2 Valid)	1
☐	12/3/2016 7:07 PM	aafdasklfasdopuqwerpouadflouooykgdt:ajsfdhkjpustf	3 (2 Valid)	1
☐	12/3/2016 7:07 PM	aafdasklfasdopuqwerpouadflouooykgdt:ajsfdhkjpustf	3 (2 Valid)	1

5

Certificate enrollment via SCEP protocol

As part of Trust Protection Platform, the VEDSCEP application server manages certificate signing requests (CSR) and renewals for Simple Certificate Enrollment Protocol (SCEP) certificates. SCEP certificates protect network mobile devices that are SCEP-enabled.

An external SCEP client, such as a network device or testing tool like SSCEP, can perform the following functions:

- Initiate a certificate enrollment.

The VEDSCEP server accepts a PKCS #10 certificate signing request (CSR).

- Request a certificate renewal.

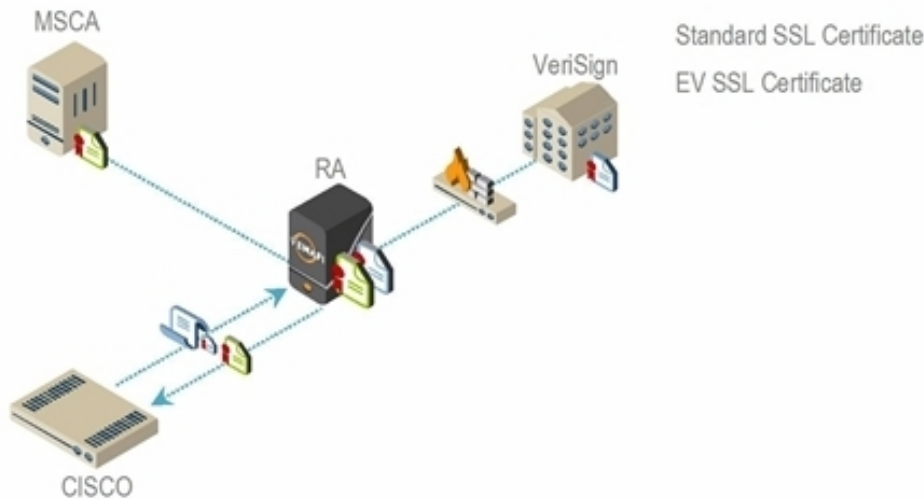
The renewal requests are signed by prior (expiring) certificate.

- Retrieve a CA and RA certificate from the VEDSCEP server.

For example, a SCEP client initiates enrollment requests to the VEDSCEP server. VEDSCEP creates certificate objects in Trust Protection Platform and marks them to be worked on by the system. The VEDSCEP server acts as an intermediary registration authority (RA) to the CA that signs certificates. The signed and encrypted format is PKCS #7.

Trust Protection Platform manages requests based on one or more CA templates. The CA must support CSR requests that do not need prior authorization.

For example, Trust Protection Platform can enroll both standard and EV SSL certificates with the Symantec MPKI CA. Additional NDE settings manage enrollment, certificate retrieval, and provisioning to the SCEP device.



Tell me more...

When initiating a request, the SCEP client must provide the correct VEDSCEP URL. If only one CA services SCEP enrollments, the URL is `http://VED_server_address/vedscep/`. For multiple CAs and CA templates, the SCEP client sends the base URL plus a CA identification string. The CA identifier is available from the Policy Tree CA template.

When the VEDSCEP receives an initial GET CA request from a network device, it returns the corresponding CA root certificate chain and its own RA certificate. The RA certificate is a Trust Protection Platform signing certificate for the enrollment CA. In practice, the RA certificate can be a standard Web certificate. The only requirement is that the certificate must be signed by the enrollment CA. If you are managing certificate enrollment with multiple CAs, you must have a separate RA certificate for each CA. The RA certificate is used as a credential to validate the identity of the RA server. Both the SCEP device and the enrollment CA require the RA certificate before they can trust the Trust Protection Platform server as the intermediary agent in the certificate enrollment process.

When Trust Protection Platform receives the subsequent enrollment request, it first creates the Certificate object in the Policy tree, then submits the CSR to the appropriate CA for enrollment. After the CA signs the certificate, Trust Protection Platform retrieves the certificate from the CA, then returns the certificate to the SCEP device.

This chapter contains the following topics:

Configuring SCEP support on Trust Protection Platform	268
Configuring network device enrollment	269
Using a policy to configure NDE	287

Configuring SCEP support on Trust Protection Platform

Trust Protection Platform uses its own built-in VEDSCEP application server to manage Simple Certificate Enrollment Protocol (SCEP) certificates. When VEDSCEP receives an initial GET CA request from a network device, it returns the corresponding CA root certificate chain and its own registration authority (RA) certificate.

When Trust Protection Platform receives the subsequent enrollment request, it first creates the certificate object in the Policy tree and then submits the certificate signing request (CSR) to the appropriate certificate authority (CA) for enrollment. After the CA signs the certificate, Trust Protection Platform retrieves the certificate from the CA and then returns the certificate to the SCEP device.

So, as part of SCEP configuration, you must configure both NDE and CA templates.

NOTE Before you begin this task, make sure you have *View* and *Write* permissions to the Policy object where you want to define the NDE settings.

To configure NDE

1. From the [Platform menu bar](#), click Policy Tree.
2. In the **Policy** tree, do the following:
 - a. Create a policy object that can be used to hold the SCEP certificates.

TIP Take some thought about the storage location for certificates in the Policy tree. By default, the policy object you specify in the NDE settings is the location where Trust Protection Platform stores certificate objects for each certificate enrolled using that CA. For more information, see ["Using a policy to configure NDE"](#) on page 287.

- b. Create at least one CA template.

If you want multiple CAs, you must define a separate CA template for each CA. For more information, see [Creating CA template objects](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

- c. (Optional) Define a credential policy for each CA .
 - d. Define a credential policy for the RA.

NOTE The RA certificate is a Trust Protection Platform signing certificate for the enrollment CA. In practice, the RA certificate can be a standard Web certificate. The only requirement is that the certificate must be signed by the enrollment CA. If you are managing certificate enrollment with multiple CAs, you must have a separate RA certificate for each CA. The RA certificate is used as a credential to validate the identity of the RA server. Both the SCEP-enabled device and the enrollment CA require the RA certificate before they can trust the Trust Protection Platform server as the intermediary agent in the certificate enrollment process.

3. (Optional) On the root **Platforms** tree, click the **Network Device Enrollment** tab, and then configure the **Default CA** and **One-Time Challenge** sections.

Add the appropriate policy settings. For more information, see ["Network device enrollment settings—Platforms and Server object"](#) on page 277.

4. On the Server object's **Network Device Enrollment** tab, add the appropriate settings.

For more information, see ["Network device enrollment settings—Platforms and Server object"](#) on page 277.

5. To manage the storage location for certificates, click the **Rules** tab and configure rules.

For more information, see ["About Network Device Enrollment rules"](#) on page 283.

6. To test certificate generation, install a SCEP client tool such as `sscep`. For more information, see our support article, [How to Setup to work with Network Device Enrollment](#).

- If there is only one CA, use the base VEDSCEP URL. For example, `http://VED_server_address/vedscep/`.
- For multiple CAs, use the base VEDSCEP URL and the **CA Ident** value from the Policy object.
- If you designated a credential and rules to store certificates in a special folder, append the folder and the credential to the VEDSCEP URL.

Configuring network device enrollment

Both the Platforms tree and Server object contain *Network Device Enrollment* tabs where you can set default parameters to manage Simple Certificate Enrollment Protocol (SCEP) certificates.

NOTE To complete this task, you must have *View* and *Write* permissions to the Trust Protection Platform server object.

To configure NDE from the Trust Protection Platform server object

1. From the **Platform menu bar**, click Policy Tree.
2. From the **Tree** drop-down menu, click the **Platforms** tree, and then click the Trust Protection Platform server object.
3. Click the **Network Device Enrollment** tab.
4. Refer to the following table while completing the configuration:

Field	Policy	Description
Settings tab		
General		
Description	n/a	Available for both Platforms and the Server object. The description for the NDE service for the Trust Protection Platform server object.
Contact		Available for both Platforms and the Server object. The user or group Identities assigned to the Network Device Enrollment Service (NDES). Administrators may reference this contact when configuring Notification Rules to provide notification for NDE events. The default contact is the master administrator.
Certificate Origin		The value to be used as the friendly name of the system requesting the certificates. It is used for reporting purposes only. The friendly name will automatically receive the SCEP prefix. For example, if you enter AirWatch, then the Certificate Origin will appear in Trust Protection Platform as SCEP-AirWatch.
Compatibility		

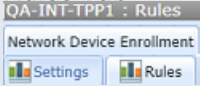
Field	Policy	Description
Issue Certificate for Identical SCEP Requests	n/a	Enabling this option allows SCEP clients to re-enroll certificates with the same private key used in the initial enrollment. Usually, this is needed when Cisco devices are used, and private key regeneration is not set. If you use this, you must also enable the SCEP Reply Delay option.
SCEP Reply Delay	n/a	Available only for the Trust Protection Platform Server object. Enabling this option delays the response time until the certificate finishes the enrollment process and it helps ensure compatibility. Some SCEP implementations do not support the <i>Pending</i> status.

Default CA

Default Challenge Password		Available for both Platforms and Server objects. The default password credential is used by SCEP-enabled devices to authenticate with the Trust Protection Platform server. The value can also be used for CA-specific enrollments that do not include a challenge password. To include the value as part of the default SCEP URL, enable Match Challenge Password to folder .
Default Certificate Container		Available for both Platforms and the Server object. The default Policy folder to hold Certificate objects for SCEP certificates. This setting applies when both conditions are met: - There are no overriding NDE rules enabled in the Policy tree. - The SCEP-enabled device fails to submit the folder Distinguished Name (DN) with the challenge password.

For more information, see ["Using rules to manage SCEP Certificate objects"](#) on page 284.

Field	Policy	Description
Default Certificate Authority		Available for both Platforms and the Server object. The Certificate Authority (CA) Template object to process all enrollment requests submitted at the default URL. The CA Template object provides the information for SCEP to submit CSRs and retrieve certificates from the CA. For more information about CA Template objects, see Certificate Authority template overview.
RA Certificate Credential		This is the registration authority (RA) certificate. The RA certificate links the current RA certificate credential to certificates in the <i>default certificate container</i>. The RA certificate is submitted to SCEP-enabled devices in response to a GET CA and to the issuing CA when submitting an enrollment request. ◦ You must have <i>view</i>, <i>read</i>, and <i>Private Key read</i> permissions to the certificate object to select it in the Certificate Selector dialog. ◦ Trust Protection Platform must have a copy of the RA certificate private key. This setting is configurable from either the Platforms or Server objects.
RA Signing Certificate Credential		Depending on whether you specified a single combined certificate or a separate Signing and Encryption certificate, select this credential, which should be linked to the RA signing certificate. specifies a single combined certificate or a separate Signing and Encryption certificate. This setting is configurable from either the Platforms or Server objects.

Field	Policy	Description
RA Encryption Certificate Credential		Select this credential, which should be linked to the RA encryption certificate. This setting is configurable from either the Platforms or Server objects.
One-Time Challenge		
Authorized Users/Groups		Available for both Platforms and the Server object. The Network Device Enrollment Service (NDES) identity user or groups.
Maximum # of challenges		Available for both Platforms and the Server object. The number of NDES password challenge attempts.
Challenge validity time		Available for both Platforms and the Server object. The number of minutes that each challenge is valid.
Rules Tab 		Available only for the Trust Protection Platform Server object. The rules are listed in order of precedence.
Configured SCEP Rules		Use to add SCEP rules. The default rule requires you to define a Folder DN as the container to hold certificates from the SCEP.
Settings		A set of checkboxes that represent rules.
Match X.509 Subject to existing certificate object	n/a	The rule with the highest priority. Overrides all other settings. Applies to certificates enrolled both at the default SCEP URL and CA-specific URLs. Trust Protection Platform does one of the following: ◦ If the Certificate object exists anywhere in the Policy tree, Trust Protection Platform uses that Certificate object in its current folder and disregards all other NDE rules. ◦ If there is no match for the certificate CA, Trust Protection Platform enrolls the certificate based on the CA settings in the server object.

Field	Policy	Description
		◦ If the existing certificate CA fails to match the CA value from the SCEP enrollment request, Trust Protection Platform enrolls the certificate with the CA specified in the SCEP enrollment request. ◦ If the Certificate object is missing from the Policy tree, Trust Protection Platform creates the Certificate object in the Policy tree.
TIP To block certificate renewal without the knowledge of the SCEP device, use the Certificate setting called Disable Automatic Renewal. For more information, see "About certificate object settings" on page 146.		
Limit certificate objects by CA ident	n/a	This is a sub-option that is available when Match X.509 Subject to existing certificate object is enabled. This sub-option restricts the search for the existing certificate object to the corresponding policy folder only, based on the CA ident included in the SCEP enrollment request.
Accept container in challenge password	n/a	The rule to allow the SCEP-enabled device to include a folder DN with the challenge password (default_password:folder_DN) as part of the request to Trust Protection Platform: ◦ Overrides the default certificate folder in the Policy object,

Field	Policy	Description
		CA-specific folders defined in folder, and all NDE folder rules defined in folder. Can only contain the default password. If the SCEP-enabled device submits a folder_DN with a CA-specific challenge password instead of the default password, Trust Protection Platform ignores the folder_DN. For example, to create Certificate objects in the NonCorp policy, SCEP request includes: <i>default_password:\Policy\NonCorp</i>
Allow X.509 Subject container rules	n/a	This rule overrides Challenge Password rules defined in the folder. Shows and enables X.509 Subject rules that are defined on this tab. The X.509 Subject rules: - Match certificates to specific policy folders based on CSR-related criteria such as Common Name, Organization, Organizational Unit, or City. - Apply only to certificates enrolled at the default URL: http(s)://VED_server_address/vedscep/. - Ignore when a CSR is submitted at a CA-specific URL. After you allow this rule-type, you must define the rule criteria in the folder where you want Trust Protection Platform to create Certificate objects for SCEP certificates. For more information, see "Using rules to manage SCEP Certificate objects" on page 284.
Match challenge password to container	n/a	The rule to enable the Challenge Password rules that are defined on this tab.

Field	Policy	Description
		Challenge Password rules match the challenge password set on a Policy object with the challenge password provided in a SCEP enrollment request submitted at Trust Protection Platform's default SCEP URL (<code>http(s)://VED_server_address/vedscep/</code>). Challenge Password rules defined in folder apply <i>only</i> to certificates enrolled at the default URL: <code>http(s)://VED_server_address/vedscep/</code>. Trust Protection Platform ignores Challenge Password rules if a CSR is submitted at a CA-specific URL. After you allow this rule-type, you must define unique challenge passwords in the folder where you want Trust Protection Platform to create Certificate objects for SCEP certificates. After you define your challenge passwords in the Policy tree, you then configure your SCEP devices to use the challenge password that corresponds to the Policy object where you want to create its corresponding Certificate object.
Support additional CAs configured on policies	n/a	The rule to allow multiple CA templates for SCEP. The Trust Protection Platform server reads both the CA template settings and the default CA settings defined in server object. If this rule is disabled, multiple CA template settings are ignored. Trust Protection Platform uses only the Default CA configuration in the server object and SCEP enrollment requests can only be submitted at the default SCEP URL.

5. Configure the NDE settings on the Server object, and then click **Save**. For more information, see "Network device enrollment settings—Platforms and Server object" on the facing page.

CAUTION If you change the NDE settings in the Trust Protection Platform Server object, the changes take effect after the VEDScep application pool is recycled. Either recycle the VEDScep application pool in IIS or issue the `iisreset/restart` command.

6. To create rules for enrollment and certificate object storage, see "Using rules to manage SCEP Certificate objects" on page 284.

After you define the default CA parameters, SCEP-enabled devices can connect with the Trust Protection Platform server at the default SCEP URL: `http(s)://VED_server_address/vedscep/`.

Network device enrollment settings—Platforms and Server object

You can set rules for managing Simple Certificate Enrollment Protocol (SCEP) certificates for network device enrollment (NDE)-enabled devices. In the root Platforms and the Server object, these tabs provide the credentials to enroll the device, and settings to store the certificate in Trust Protection Platform.

You can also set policy rules for managing the certificates in a container or policy folder. For more information, see "Using a policy to configure NDE" on page 287.

Trust Protection Platform has the ability to emulate a Microsoft NDES server. This allows Trust Protection Platform to be compatible with all SCEP clients that have out-of-the-box compatibility with Microsoft NDES servers. Example URLs:

- SCEP certificate enrollment: *https://[Trust Protection Platform Server]/certsrv/mscep*
- SCEP one-time challenge passphrase: *https://[Trust Protection Platform Server]/certsrv/mscep_admin*

NOTE If you change the NDE settings in the Trust Protection Platform server object, the changes are not effective until the SCEP application pool is recycled. Either recycle the VEDScep application pool in IIS or issue the `iisreset/restart` command.

NOTE Previous versions of Trust Protection Platform contained the Enable AirWatch Workaround option. This option is no longer needed. Instead, when AirWatch is used, we recommended specifying both **RA Signing Certificate Credential** and **RA Encryption Certificate Credential** instead of only **RA Certificate Credential**.

Field	Policy	Description

Settings tab

General

Description	n/a	Available for both Platforms and the Server object. The description for the NDE service for the Trust Protection Platform server object.

Contact		Available for both Platforms and the Server object. The user or group Identities assigned to the Network Device Enrollment Service (NDES). Administrators may reference this contact when configuring Notification Rules to provide notification for NDE events.

Field	Policy	Description
The default contact is the master administrator.		
Certificate Origin		The value to be used as the friendly name of the system requesting the certificates. It is used for reporting purposes only. The friendly name will automatically receive the SCEP prefix. For example, if you enter AirWatch, then the Certificate Origin will appear in Trust Protection Platform as SCEP-AirWatch.
Compatibility		
Issue Certificate for Identical SCEP Requests	n/a	Enabling this option allows SCEP clients to re-enroll certificates with the same private key used in the initial enrollment. Usually, this is needed when Cisco devices are used, and private key regeneration is not set. If you use this, you must also enable the SCEP Reply Delay option.
SCEP Reply Delay	n/a	Available only for the Trust Protection Platform Server object. Enabling this option delays the response time until the certificate finishes the enrollment process and it helps ensure compatibility. Some SCEP implementations do not support the <i>Pending</i> status.
Default CA		
Default Challenge Password		Available for both Platforms and Server objects. The default password credential is used by SCEP-enabled devices to authenticate with the Trust Protection Platform server. The value can also be used for CA-specific enrollments that do not include a challenge password. To include the value as part of the default SCEP URL, enable Match Challenge Password to folder.
Default Certificate Container		Available for both Platforms and the Server object. The default Policy folder to hold Certificate objects for SCEP certificates. This setting applies when both conditions are met: There are no overriding NDE rules enabled in the Policy tree.

Field	Policy	Description
		▪ The SCEP-enabled device fails to submit the folder Distinguished Name (DN) with the challenge password. For more information, see "Using rules to manage SCEP Certificate objects" on page 284.
Default Certificate Authority		Available for both Platforms and the Server object. The Certificate Authority (CA) Template object to process all enrollment requests submitted at the default URL. The CA Template object provides the information for SCEP to submit CSRs and retrieve certificates from the CA. For more information about CA Template objects, see Certificate Authority template overview.
RA Certificate Credential		This is the registration authority (RA) certificate. The RA certificate links the current RA certificate credential to certificates in the <i>default certificate container</i>. The RA certificate is submitted to SCEP-enabled devices in response to a GET CA and to the issuing CA when submitting an enrollment request. ▪ You must have <i>view</i>, <i>read</i>, and <i>Private Key read</i> permissions to the certificate object to select it in the Certificate Selector dialog. ▪ Trust Protection Platform must have a copy of the RA certificate private key. This setting is configurable from either the Platforms or Server objects.
RA Signing Certificate Credential		Depending on whether you specified a single combined certificate or a separate Signing and Encryption certificate, select this credential, which should be linked to the RA signing certificate.

Field	Policy	Description
		specifies a single combined certificate or a separate Signing and Encryption certificate. This setting is configurable from either the Platforms or Server objects.
RA Encryption Certificate Credential		Select this credential, which should be linked to the RA encryption certificate. This setting is configurable from either the Platforms or Server objects.
One-Time Challenge		
Authorized Users/Groups		Available for both Platforms and the Server object. The Network Device Enrollment Service (NDES) identity user or groups.
Maximum # of challenges		Available for both Platforms and the Server object. The number of NDES password challenge attempts.
Challenge validity time		Available for both Platforms and the Server object. The number of minutes that each challenge is valid.
Rules Tab 		Available only for the Trust Protection Platform Server object. The rules are listed in order of precedence.
Configured SCEP Rules		Use to add SCEP rules. The default rule requires you to define a Folder DN as the container to hold certificates from the SCEP.
Settings		
Match X.509 Subject to existing certificate object	n/a	The rule with the highest priority. Overrides all other settings. Applies to certificates enrolled both at the default SCEP URL and CA-specific URLs. Trust Protection Platform does one of the following: ■ If the Certificate object exists anywhere in the Policy tree, Trust Protection Platform uses that Certificate object in its current folder and disregards all other NDE rules.

Field	Policy	Description
		■ If there is no match for the certificate CA, Trust Protection Platform enrolls the certificate based on the CA settings in the server object. ■ If the existing certificate CA fails to match the CA value from the SCEP enrollment request, Trust Protection Platform enrolls the certificate with the CA specified in the SCEP enrollment request. ■ If the Certificate object is missing from the Policy tree, Trust Protection Platform creates the Certificate object in the Policy tree.
TIP To block certificate renewal without the knowledge of the SCEP device, use the Certificate setting called Disable Automatic Renewal. For more information, see "About certificate object settings" on page 146.		
Limit certificate objects by CA ident	n/a	This is a sub-option that is available when Match X.509 Subject to existing certificate object is enabled. This sub-option restricts the search for the existing certificate object to the corresponding policy folder only, based on the CA ident included in the SCEP enrollment request.
Accept container in challenge password	n/a	The rule to allow the SCEP-enabled device to include a folder DN with the challenge password (default_password:folder_DN) as part of the request to Trust Protection Platform:

Field	Policy	Description
		- Overrides the default certificate folder in the Policy object, CA-specific folders defined in folder, and all NDE folder rules defined in folder. - Can only contain the default password. If the SCEP-enabled device submits a folder_DN with a CA-specific challenge password instead of the default password, Trust Protection Platform ignores the folder_DN. For example, to create Certificate objects in the NonCorp policy, SCEP request includes: <i>default_password:\Policy\NonCorp</i>
Allow X.509 Subject container rules	n/a	This rule overrides Challenge Password rules defined in the folder. Shows and enables X.509 Subject rules that are defined on this tab. The X.509 Subject rules: - Match certificates to specific policy folders based on CSR-related criteria such as Common Name, Organization, Organizational Unit, or City. - Apply only to certificates enrolled at the default URL: http(s)://VED_server_address/vedscep/. - Ignore when a CSR is submitted at a CA-specific URL. After you allow this rule-type, you must define the rule criteria in the folder where you want Trust Protection Platform to create Certificate objects for SCEP certificates. For more information, see "Using rules to manage SCEP Certificate objects" on page 284.
Match challenge password to container	n/a	The rule to enable the Challenge Password rules that are defined on this tab.

Field	Policy	Description
		Challenge Password rules match the challenge password set on a Policy object with the challenge password provided in a SCEP enrollment request submitted at Trust Protection Platform's default SCEP URL (<code>http(s)://VED_server_address/vedscep/</code>). Challenge Password rules defined in folder apply <i>only</i> to certificates enrolled at the default URL: <code>http(s)://VED_server_address/vedscep/</code>. Trust Protection Platform ignores Challenge Password rules if a CSR is submitted at a CA-specific URL. After you allow this rule-type, you must define unique challenge passwords in the folder where you want Trust Protection Platform to create Certificate objects for SCEP certificates. After you define your challenge passwords in the Policy tree, you then configure your SCEP devices to use the challenge password that corresponds to the Policy object where you want to create its corresponding Certificate object.
Support additional CAs configured on policies	n/a	The rule to allow multiple CA templates for SCEP. The Trust Protection Platform server reads both the CA template settings and the default CA settings defined in server object. If this rule is disabled, multiple CA template settings are ignored. Trust Protection Platform uses only the Default CA configuration in the server object and SCEP enrollment requests can only be submitted at the default SCEP URL.

About Network Device Enrollment rules

For large numbers of SCEP-enrolled certificates, you create policy-based rules from the Platforms Server object **Network Device Enrollment Rules** tab.

Network Device Enrollment (NDE) rules are based on Certificate Signing Request (CSR) Subject criteria or the Challenge Password. If the CSR contains the VEDSCEP default SCEP URL that matches an NDE rule, Trust Protection Platform creates the Certificate object under the corresponding Policy object.

Trust Protection Platform also provides a rule that attempts to match CSR subject criteria to existing Certificate objects in the Policy tree before it creates a new Certificate object.

For example, the Match X.509 Subject to Existing Certificate object rule performs these actions:

- Before attempting to create the Certificate object in response to the enrollment request, Trust Protection Platform looks for a corresponding Certificate object in the Policy tree.
- Based on what it finds, Trust Protection Platform does one of the following:
 - If the Certificate object exists anywhere in the Policy tree, Trust Protection Platform uses that Certificate object in its current folder and disregards all other NDE rules.
 - If the certificate exists but the CA configured in the Certificate object does not match the CA configured for the SCEP enrollment request, Trust Protection Platform enrolls the certificate with the CA configured in the Trust Protection Platform server object.
 - If the Certificate object does not exist in the tree, Trust Protection Platform creates the Certificate object.
- When the **Match X.509 Subject to existing certificate object** setting is enabled, you also have the option to limit certificate objects by CA ident, which restricts the search for the existing certificate object to the corresponding policy folder only, based on the CA ident included in the SCEP enrollment request.

Using rules to manage SCEP Certificate objects

You can use rules to control inbound Simple Certificate Enrollment Protocol (SCEP) requests. The rules manage the certificate storage location in Trust Protection Platform based on the request content, existing certificate information, or CA configuration settings.

To create rules for SCEP Certificate object storage

1. From the [Platform menu bar](#), click Policy Tree.
2. Navigate to **Platforms** and click the server object.
3. Click the **Network Device Enrollment** tab, and then click the **Rules** tab.
4. Click **Add**.

5. To store the SCEP Certificate objects in a Policy folder, set the **Container** and select **Use Container if** certificate criteria.
6. (Optional) In the **Certificate Origin** field, enter the friendly name to be used when new SCEP Certificate objects are added to Trust Protection Platform. The object name will automatically receive the SCEP prefix when created.
7. (Optional) To require an additional **Challenge Password** for storage on the Policy folder, select a Password Credential. If the credential is the same as the **Default Challenge Password** that you specified in the **Platforms NDE** tab, the rule is ignored.
8. (Optional) To override the Default CA, type a **CA Ident** string, select a **Certificate Authority**, which is a CA template, and then set the **RA Certificate Credential**.
9. (Optional) Enable **Match X.509 Subject to existing certificate object** to use the same certificate object for renewal requests. This means that if a customer enrolls a certificate via SCEP and then, a year later, requests SCEP again, the system will attempt to match the existing certificate object using the CSR's Subject, provided this option is enabled. If the option is disabled, the system will simply create a new object.

The screenshot shows a 'Settings' panel with the following options:

- Match X.509 Subject to existing certificate object: ☒
- Use CA ident to match to certificate object: ☐
- Accept container in challenge password: ☒
- Allow X.509 Subject container rules: ☒
- Match challenge password to container: ☐
- Support additional CAs configured on policies: ☐

When you enable this option, you will have the sub-option (not shown) to **Limit certificate objects by CA ident**, which restricts the search for the existing certificate object to the corresponding policy folder only, based on the CA ident included in the SCEP enrollment request.

10. Click **Save**.
11. In the Settings section, enable or disable rules. Use the following chart to determine the appropriate check boxes for managing SCEP rules
 - To enable and show rules, select the appropriate check boxes, and then click **Save**.
 - To disable and hide rules, clear the appropriate check boxes, and then click **Save**.

- To require the challenge password to manage the certificate storage location, select **Match Challenge Password to folder**.
- To require both a challenge password and the folder Distinguished Name (DN) to manage the certificate storage location, select **Accept folder in Challenge Password**.

If you defined this rule... Enable or disable the rule with this check box		Corresponding SCEP Rule Type
Container	Match X509 Subject to existing certificate object	Provided Container
Challenge Password	Accept container in challenge password	Select via Password
Challenge Password	Match challenge password to container	Select via Password
Use Container if	Allow X.509 Subject container rules	Subject Match
Default CA (all settings)	Support additional CAs configured on policies	CA Ident URL

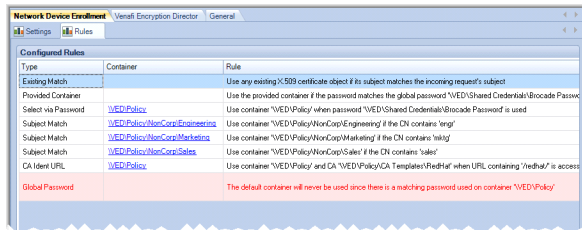
12. In the Configured SCEP Rules section, correct any rules that appear in red text, and then click **Save**.

Example of rule execution

The execution of rules are defined on the Server object **Network Device Enrollment Rules** tab. The hierarchical, policy-based rules allow administrators to manage the destination for Certificate objects in the Policy tree.

The **Rules** tab only lists enabled Simple Certificate Enrollment Protocol (SCEP) rules. The rules apply to the Policy tree and those defined on the Server object. In this example:

- Five rules are enabled, and partial matches on the Common Name (CN) in the Certificate Signing Request (CSR) are configured on three folders in the Policy tree.
- The rules are listed in order of precedence.
- Rules of the same type are executed in alphanumeric order by *Container*. In the example, the *Subject Match* rules sort first, \VED\Policy\NonCorp\Engineering, then \VED\Policy\NonCorp\Marketing, and lastly \VED\Policy\NonCorp\Sales.
- Any rules, highlighted in red, will not be executed with the current configuration. The reason the rule would not be executed will be noted in the **Rule** column. In this example, the *Global Password* rule would not ever execute because the same challenge password is assigned at the \VED\Policy folder object.



The rules are displayed in the order they are executed. When a rule is found that matches the conditions of the CSR, execution ends and the matching rule is applied. Rules are applied in the following order:

1. Match X.509 Subject to existing certificate object. When enabled, you have the option to limit certificate objects by CA ident, which restricts the search for the existing certificate object to the corresponding policy folder only, based on the CA ident included in the SCEP enrollment request.
2. Accept folder in challenge password
3. Allow X.509 Subject folder rules.
4. Match challenge password to container
5. Support additional CAs configured on policies

NOTE If a **CA Ident** string is configured on a Policy object and the value is sent as part of the SCEP request from the device, only the first two rules in this list are processed. No X.509 subject folder rules or challenge password match rules will be processed. Additionally, if a folder challenge password is provided on the folder along with the **CA Ident** value, only that challenge password will be used in determining if a valid SCEP request has been sent by the device.

Using a policy to configure NDE

You can use rules on a Policy object to manage network device enrollment (NDE) for Simple Certificate Enrollment Protocol (SCEP) certificates. If you are using multiple CA templates, you can create a Policy object for each CA.

You must have *View* and *Write* permissions to the Policy object where you want to define NDE settings.

NOTE If you change the NDE settings on the Policy object, the changes are not effective until the SCEP application pool is recycled. Either recycle the VEDSCEP application pool in IIS or issue the `iisreset/restart` command.

To configure the NDE settings on the Policy object

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** object.
4. Click the **Network Device Enrollment** tab. Refer to the following table while completing the configuration:

Network Device Enrollment settings

Field	Policy	Description
General		
Challenge Password		(Optional) Requires you to enable the Accept container in challenge password on the Server object Rules tab. The challenge password associated with the current Policy object. If this field is empty, the SCEP-enabled device uses the Platform Default Challenge Password in the URL. For more information, see "Network device enrollment settings—Platforms and Server object" on page 277. The Policy Challenge Password is: ◦ A credential to enroll certificates at the CA-specific URL. The URL is created using the Policy object CA Ident string. ◦ Part of the Use container if rule.
Use container if	n/a	(Optional) A rule to determine whether to create the Certificate object for a SCEP-enrolled certificate under the current Policy object. To confirm that the rule does not offer duplicate challenge passwords, see "Example of rule execution" on page 286.

Field	Policy	Description
		- Set the Allow X.509 Subject folder Rules option on the Trust Protection Platform server object. Otherwise, the rule is ignored. For more information, see "Example of rule execution" on page 286. - Set a field value. Field values include Any X.509 field, Common Name, Organization, Organizational Unit, and City. - Set a comparison operator. Operator values include starts with, matches or contains.

For example, this rule creates the associated Certificate object under the current Policy object after a SCEP-enabled device submits a CSR that included "NonCorp" in its Organization string.

Certificate Origin	n/a	The value to be used as the friendly name of the system requesting the certificates. It is used for reporting purposes only. The friendly name will automatically receive the SCEP prefix. For example, if you enter AirWatch, then the Certificate Origin will appear in Trust Protection Platform as SCEP-AirWatch.
Default CA		
CA Ident	n/a	An identification string that is appends to Trust Protection Platform base SCEP URL to create a CA-specific URL.

Field	Policy	Description
		For example, if the value is <i>redhat</i> , the CA URL where SCEP devices can enroll certificates is http://scep.example.com/vedscep/redhat/ .
Certificate Authority	n/a	The CA Template object that Trust Protection Platform uses to: ◦ Enroll certificates submitted at the URL created with the CA Ident string. ◦ Connect to the CA and submit CSRs. ◦ Post the certificate CSR. ◦ Retrieve certificates from the CA.

Field	Policy	Description
RA certificate credential	n/a	This is the registration authority (RA) certificate. The RA certificate links the current RA certificate credential to certificates in the <i>default certificate container</i>. The RA certificate is submitted to SCEP-enabled devices in response to a GET CA and to the issuing CA when submitting an enrollment request. ◦ You must have <i>view</i>, <i>read</i>, and <i>Private Key read</i> permissions to the certificate object to select it in the Certificate Selector dialog. ◦ Trust Protection Platform must have a copy of the RA certificate private key. This setting is configurable from either the Platforms or Server objects.
RA Signing Certificate Credential		Select this credential, which should be linked to the RA signing certificate. This setting is configurable from either the Platforms or Server objects.
RA Encryption Certificate Credential		Select this credential, which should be linked to the RA signing certificate. This setting is configurable from either the Platforms or Server objects.

5. Configure **General** and **Default CA** settings, and then click **Save**.

6

Managing local certificates

Venafi Trust Protection Platform™ enables organizations to scan their network's local file systems and keystores to build an inventory of local certificates. Trust Protection Platform discovers all end-entity certificates as well as root and intermediate root certificates.

After you discover your local certificates, you can bring those certificates under management. You can define local certificate folders to enforce certificate compliance and receive notifications of certificate expiration.

This chapter contains the following topics:

About self-signed certificates in Trust Protection Platform	294
Configuring certificate objects	302
About local certificate settings	303
About a certificate's summary (Policy Tree)	311
About Viewing Certificate History	313
Revoke historical certificates	314

Revert historical certificates	315
Download historical certificates	316
Managing Local Certificates Via Policy	317
Policy object certificate settings	319
Policy object monitoring settings	327
Using PBE (password-based encryption) algorithms to secure private keys	329
Determining certificate compliance	330

About self-signed certificates in Trust Protection Platform

A self-signed certificate is an identity certificate that is signed by the same person or organization whose identity it certifies. It is a certificate that is signed with its own private key.

What's the difference between a certificate issued by a Certificate Authority and a self-signed certificate?

A Certificate Authority (CA) issues a digital certificate that verifies the ownership of a public key by the named subject of the certificate. The CA is a trusted third party, trusted by both the subject (who asked to be verified) and the person doing business with the subject (who relies on the validity of the certificate).

When is it okay to use self-signed certificates?

When you're sure that self-signed certificates are accounted for and under management, they can be used on an internal network. If a CA is not required to verify the identity of the subject to a relying party, and the relying party instead chooses direct trust of the certificate, then self-signed certificates can be used.

When properly managed, self-signed certificates can be an efficient and less costly way to manage security.

What are the risks of using self-signed certificates?

In general, it is wise to be diligent when using self-signed certificates because of the inherent risk of lack of identity verification and trust control. The public and private keys are both held by the same entity.

Self-signed certificates cannot be revoked. If an attacker has already gained access to a system, the attacker can spoof the identity of the subject. CAs can revoke a certificate when they discover the compromise. Self-signed certificates cannot be revoked. They can only be replaced.

Who should be allowed to create self-signed certificates?

Self-signed certificate templates don't require any credentials to create or use. Any user with Create permissions can create a self-signed certificate template. Policy branches that do not have an enforced "certificate authority template" value can be set to use any existing certificate template object.

Trust Protection Platform administrators who want to control the use of self-signed certificates with users should review user permissions, policy settings, and workflow implementations in their environment. An example might be locking the certificate authority template that certificate objects can use at the policy level.

This chapter contains the following sections:

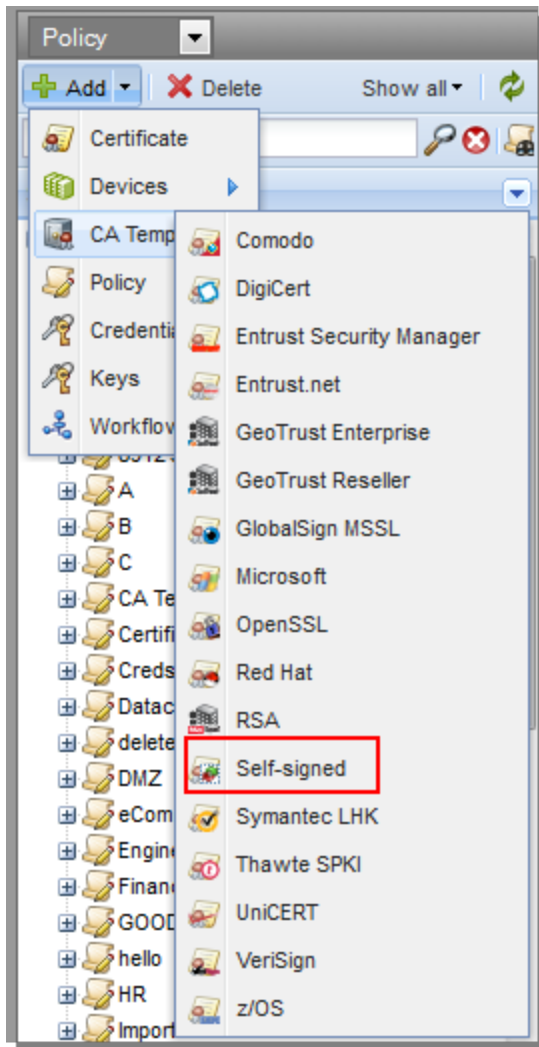
This chapter contains the following topics:

Configuring a self-signed certificate template

You must have *view* and *write* permissions on the object where you want to configure settings.

To create a self-signed certificate template

1. From the **Policy** tree, click **Add > CA Template > Self-signed**.



2. In the **General** box, give the template a **CA Name** and **Description**.

Specify a contact, if needed. In this example, our template is called *HR Self-signed certificate*:

The screenshot shows the 'Add New : Self-signed' dialog box. The 'General' tab is selected, showing the following fields:

- CA Name: HR Self-signed Cert
- Description: HR Self-signed Cert
- Contact(s):

The 'Options' tab is also visible, showing the following settings:

- Key Usage: EncipherOnly, KeyAgreement, DataEncipherment, KeyDecipherment, NonRepudiation, DigitalSignature
- Server Authentication: ☐
- Client Authentication: ☐
- Signature Algorithm: SHA256

The 'Validity Period' tab is also visible, showing the following settings:

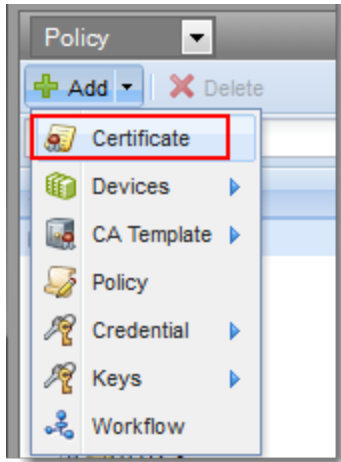
- Years: 1
- Days: 0

3. In the **Options** box, select:
 - a. Key Usage: Select the appropriate key usage.
 - i. (Optional) Server Authentication: Enhancement to Key Usage
 - ii. (Optional) Client Authentication: Enhancement to Key Usage
 - b. Signature Algorithm: The default is SHA256.
4. In the **Validity Period** box, specify how long the certificate will be valid.

The maximum period is 5 years.
5. Click **Save**.

To create a self-signed certificate using the Self-signed Certificate template

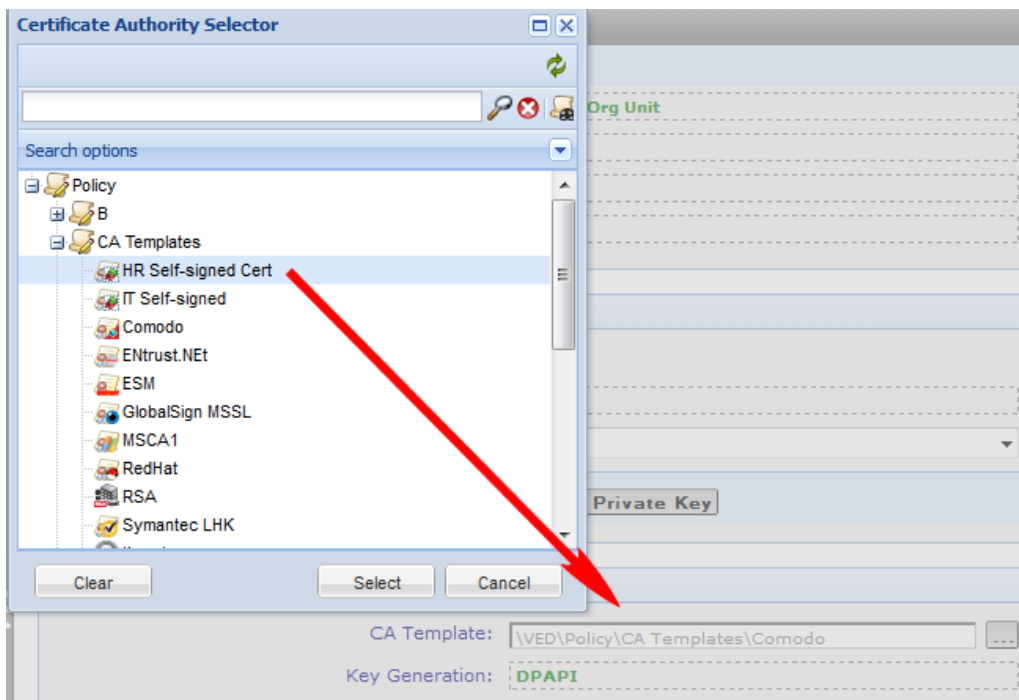
1. In Policy, click **Add** , and then click **Certificate**.



2. In the **General Information** box, fill in the **Certificate Name** and **Description**.
3. Verify that the Contact and Approver names are correct.
4. Set the **Management Type** to either Monitored, Enrollment, Provisioned, or Unassigned.

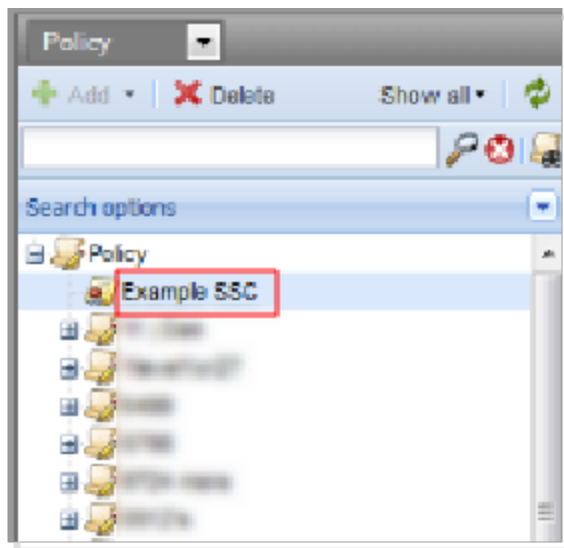
A screenshot of the 'General Information' box in the Venafi Trust Protection Platform. The box contains several fields: 'Certificate Name' (Example SSC), 'Description' (Example SSC), 'Contact(s)' (local:Admin (\VED\Identity\Admin)), 'Approver(s)' (local:Admin (\VED\Identity\Admin)), 'Processing Disabled' (checkbox), and 'Management Type' (Enrollment). The 'Certificate Name' and 'Management Type' fields are highlighted with red boxes. There are also icons for adding and editing on the right side of the box.

5. Fill out the certificate information.
6. In the **Other Information** box, the CA Template should be set to the self-signed certificate template you created.



7. When you're done, click **Save**.

You'll see the new certificate in the Policy tree.



FAQ: Self-signed certificates

This section offers answers to commonly asked questions about self-signed certificates.

How does Trust Protection Platform identify a self-signed certificate?

For a certificate to be *self-signed*, the following must be true (as shown in **Certificate Details**):

- The Subject DN and the Issuer DN are the same *and*
- Basic Constraints is set to *CA=False*

Or

Key Usage is set to one or more of the following:

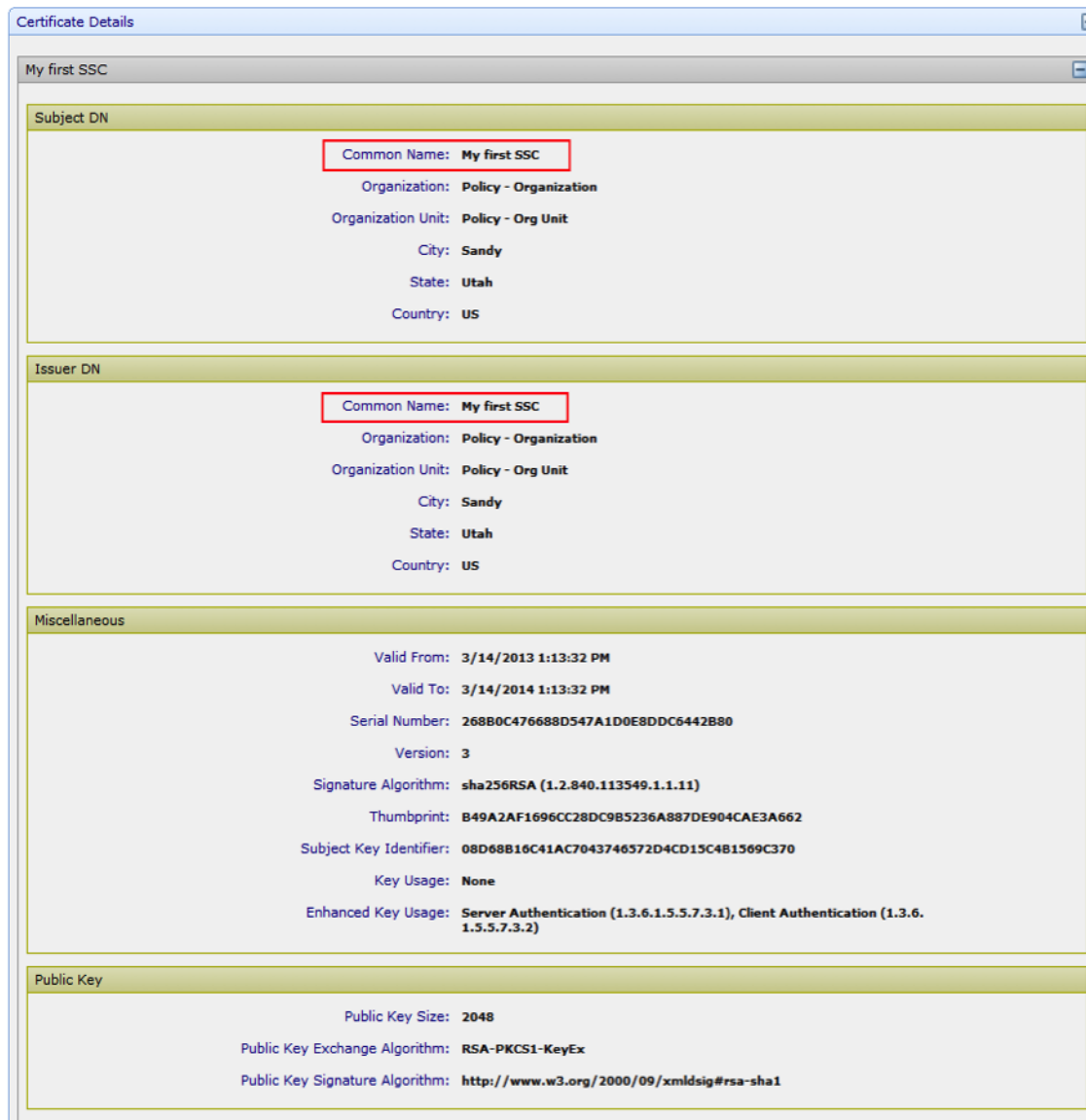
- Digital Signature
- Content Commitment
- Key Encipherment
- Data Encipherment
- Key Agreement
- Encipher Only
- Decipher Only

For a certificate to be a root certificate, the following must be true (as shown in **Certificate Details**):

- The Subject DN and the Issuer DN are the same, *and*
- Basic Constraints is set to *CA=True*.

Or

- Key usage is set to *KeyCertSign*.
- Basic Constraints and Key Usage are not used.



What happens to self-signed certificates that are currently in the Roots tree?

Existing self-signed certificates remain in the Roots tree. However, subsequent self-signed certificates cannot be placed there. They can only be placed in the Policy tree.

What happens to self-signed certificates that are identified and brought under management through agent discovery?

Self-signed Certificates are discovered and delivered to the appropriate discovery queues for review. These certificate types are changed to *self-signed*. Administrators can place self-signed certificates in the Policy tree. These certificates can no longer be placed in the Roots tree.

Can I revoke self-signed certificates?

Self-signed certificates cannot be revoked. They can, however, be renewed through the standard renewal process.

How are self-signed certificates similar to CA-issued certificates in Trust Protection Platform?

Just as you can with CA-issued certificates, you can do the following with self-signed certificates:

- Renew, import, and retrieve
- Add, remove, push, extract, enable, and retry application certificates
- Configure notifications for self-signed certificates.

Self-signed certificates are also displayed in log events, grids, and reports, in the same way CA-issued certificates are displayed.

When I look at the certificate details, under Key Usage, I see "Information Not Available." What does that mean?

Information Not Available means that the combination of key usages you chose when you set up the self-signed certificate template are incorrect. Valid combinations are displayed. But invalid combinations return *Information Not Available*.

For more information about self-signed certificates, see ["About self-signed certificates in Trust Protection Platform" on page 294](#).

Configuring certificate objects

You can change certificate settings in the Policy tree.

IMPORTANT You must have the *Write* permission to a certificate object before you can configure it.

To configure a certificate object

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. In the Policy tree, select the certificate object you want to configure.
3. Click the **Certificate > Settings** tab.
4. Complete certificate settings, and then click **Apply/Save**.

For more information, see "[About local certificate settings](#)" below in the Venafi Trust Protection Platform *Trust Protection Platform Certificate Management Guide*.

About local certificate settings

A *local certificate* is a certificate that a network scan utility retrieved from a computer's local file system. A corresponding certificate object appears in the Policy tree.

A *certificate object* is a container that holds the information Trust Protection Platform needs to monitor, enroll, or provision certificates. You can configure a certificate object's settings in a policy, or you can configure them directly on a certificate object itself. Some settings, such as domain whitelisting settings, can only be set on a policy.

BEST PRACTICE You should consider managing certificate object settings using a policy. For more information, see "[Managing Local Certificates Via Policy](#)" on page 317.

The following table only lists relevant settings for local certificate objects. The second column indicates if the setting can also be managed using Policy. If you want details about other settings, see "[About certificate object settings](#)" on page 146.

Field	Policy	Description
 Refresh	n/a	Refreshes the contents of the current page.
 Print	n/a	Prints the contents of the current Detail View.

Field	Policy	Description
Certificate Tab		
Summary Subtab		Provides an overview of the current certificate. For more information, see "About a certificate's summary (Policy Tree)" on page 311 .
Certificate Status		
Status	n/a	Current status of the Certificate object.  There is no processing and the certificate is working.  The certificate is being processed. The status field provides a description of what is happening.  There is a problem and the certificate is not functioning. The status field provides a description of the problem.
Expiration Date	n/a	The date the certificate expires.
Settings Tab		
 Download	n/a	This option is available only in Policy Tree. Downloads the certificate and, optionally, the private key and root chain from the Trust Protection Platform database and allows you to save it to a Base64, DER, PKCS#7, or PKCS#12 formatted file. If you select PKCS#12 format, you can define a password that will be required to access the downloaded certificate and private key. For more information, see "Downloading certificates, private keys, and root chains" on page 453.
 Import	n/a	This option is available only in Policy Tree.

Field	Policy	Description
		Allows you to copy and paste a Base64-encoded certificate file (and, optionally, the private key) into Policy Tree. Trust Protection Platform automatically populates the Certificate object with the certificate data and, when you save the Certificate object, it archives the certificate file in the Trust Protection Platform database. If the uploaded certificate includes the Private key, you must specify the password required to access the private key. You must have the View and Write permissions to the Certificate object to import a certificate. If the certificate is in a format that includes the private key, you must also have the Private Key Write permission to the Certificate object. For more information, see "Importing an existing certificate" on page 135.

General Information

Certificate Name	No	Unique name for the Certificate object. This is a mandatory field.
Description	No	Description for the Certificate 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.

Field	Policy	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, 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, discontinuous users and groups. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Management Type		Currently, Trust Protection Platform only manages local certificates at the Monitoring level. Under Monitoring, Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform notifies the administrator. It does not, however, renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then retrieve and install the renewed certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Subject DN		

Field	Policy	Description
Common Name	No	Typically, the fully qualified domain name.
Subject Alt Name	No	The DNS-based Subject Alt Name(s) (SANs) associated with the current certificate.
Organization		Name that uniquely identifies the organization in the certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Organization Unit		Department or division within the organization that is responsible for maintaining the certificate. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
City, State/Province, Country		Location (city, state/province, and country) of your Organization or Organizational Unit. You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Private Key		
Private Key Stored	No	Indicates whether Trust Protection Platform currently has a copy of the certificate's private key—Yes or No.
Key Strength (bits)		Certificate's key strength.

Field	Policy	Description
		You can manage this setting at the policy level. To configure the setting via Policy, go to the Settings > Certificate tab in the Policy object configuration. The setting defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319 .
Upload Private Key	No	Allows the administrator to paste the private key data or upload a private key file to the Trust Protection Platform database. The private key must be base64 encoded and you must specify the password required to access the private key. You must have the Private Key Write, View, and Write permissions to the Certificate object to upload a private key. For more information, see "Manually Uploading the Private Key" on page 218.

Other Information

CA Template



The CA that issued the certificate.

Trust Protection Platform does not currently enroll or provision local certificates, so this field is not required. However, you can use this field to monitor compliance with local certificate folders.

To select the CA Template object

Click the **Browse** button.

The Configuration Object Selector dialog opens.

Select a CA Template object, and then click **Select**.

For more information on CA Template objects, see [CA integration setup](#).

Field	Policy	Description
		You can manage the following settings at the policy level. To configure these settings via Policy, go to the Settings > Certificate tab in the Policy object configuration. The settings defined in the Policy object may be inherited by all subordinate Certificate objects. For more information, see "Policy object certificate settings" on page 319.
Key Generation	n/a	This option is not relevant to local certificates.
Renewal Window	n/a	This option is not relevant to local certificates.
Associations Tab	No	Lists the applications associated with the current certificate. Trust Protection Platform does not currently enroll or provision local certificates, so this field is not required. However, you can use this field to identify the platform or keystore where the local certificate is located. For more information and details about the options available in the Associations tab, see "Associating certificates with applications" on page 202.
Compliance Tab	n/a	The Compliance tab provides an assessment of the certificate's compliance with its parent folder. For more information, see "Managing Local Certificates Via Policy" on page 317.
Certificate Value	n/a	The Certificate Value column lists the certificate values as they are currently defined in the certificate. Certificate Values are listed as being in  or out  of policy.

Field	Policy	Description
Renewal Value	n/a	The Renewal Value column lists the certificate values currently defined in the Certificate object. Renewal values also reflect policy status.
History Tab	n/a	The Certificate History tab lists the common name, serial number, issuer, and valid dates for each edition of the certificate associated with the current Certificate object. Each time a new certificate is issued or an existing certificate is renewed, Trust Protection Platform adds another entry to the Certificate object's History tab. For more information, see "About Viewing Certificate History" on page 313.
Monitoring Tab		The Monitoring tab defines the parameters for certificate expiration events. The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the Channel and Notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393. You can define Monitoring settings at the policy level. To configure the Certificate object's monitoring settings, go to the Settings > Monitoring tab in the Policy object configuration. The Certificate object monitoring settings defined in the Policy object can be inherited by all subordinate Certificate objects. For more information, see "Policy object monitoring settings" on page 327.
Settings		
Disabled		Disables monitoring for the current Certificate object.
Expiration Events		
Start generating events		Number of days before a certificate expires that you want to start generating expiration events.

Field	Policy	Description
Send event every		Frequency (in days) at which you want Trust Protection Platform to generate expiration events.
Escalation Expiration Events		
Start escalating events		Number of days before a certificate expires that you want to start generating escalated expiration events.
Send event every		Frequency (in days) at which you want Trust Protection Platform to generate escalated expiration events.
General Tab		
Log Tab	n/a	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 Tab	n/a	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.

About a certificate's summary (Policy Tree)

The **Certificate > Summary** tab provides a snapshot of the current certificate. It lists the certificate status, all associated applications, the certificate signature chain, and the certificate details.

NOTE Any user with *Write* permission to the certificate can access all of the options in the Certificate Summary tab and view all summary data, including information about the certificate's associated applications regardless of whether the user has permissions to the associated applications.

Certificate Status section

The Certificate Status section contains detailed information about errors, processing, validation, and other vital details.

(Status messages) Just below the Certificate Status title bar, Trust Protection Platform displays the current status of the certificate object, including the following common messages:



There is no processing and the certificate is working.



The certificate is being processed. The status field provides a description of what is happening.



There is a problem and the certificate is not functioning. The status field provides a description of the problem.



Workflow request has been rejected.

Expiration Date

States the date and time that the certificate will expire. A value will be shown only if the certificate object has a certificate currently linked to it.

Lifecycle Stage

Processing Stage states the stage number that the certificate is currently on. Certificate will state "none" if it is not currently processing.

Revocation

Shows the date and time of the last revocation check, as well as the result of the last revocation check.

Validation

Displays the time stamp for the last network validation of the certificate. Network validation settings are controlled on the Validation tab of the certificate object.

Displays the results of the last network validation attempt for the certificate object.

Associated Applications

This section lists the applications the certificate object is associated with. It also details the current status, processing stage, and validation results of each specific associated application.

Certification Path

If a certificate is currently linked to a certificate object, Trust Protection Platform will build the root chain for the certificate and display it here.

Certificate Details

Trust Protection Platform lists all of the details of the certificate that is linked to the certificate object. All the details of each certificate in the root chain are displayed here as well.

About Viewing Certificate History

You can view certificate history to see previous versions of a certificate that has been renewed.

When you are viewing a certificate, you can open the **Previous Versions** page to see a list of previous versions of the certificate that have been replaced.



102.generated.venafi.com

Policy\Generated\Certificate 100 - 199

Actions

Overview

Installations

SSL/TLS

Previous Versions

Permissions

This list shows previous versions of the certificate which have been replaced.

Displaying 2 Previous Certificates

Common Name	Serial Number	Issuer	Valid From	Valid To	Status	
102.generated.venafi.com	1E0CB92EC094244BBB3EF92FCCA324AD	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download
102.generated.venafi.com	0DD61A394451AC4497B4A2D56857C1B6	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download

For each item in the list you can see selected information about the certificate. For complete certificate details, click on the certificate **Serial Number**.

For more details on working with historical certificates see:

- ["Revoke historical certificates" on the next page](#)
- ["Revert historical certificates" on page 315](#)
- ["Download historical certificates" on page 316](#)

Revoke historical certificates

A previous version of a certificate may still be a valid certificate, and you may decide you want to revoke it in the system. You can only revoke a certificate if the following is true:

- You have the *Revoke* permission to the certificate.
- The certificate is not "In Error."
- Another historical certificate or the current certificate is not being revoked.
- The certificate is not renewing, or installing/provisioning.
- The management type is assigned.
- The certificate is not listed as "Lost."
- The certificate is not self-signed.
- The certificate is not revoked.

Revoke a historical certificate

To revoke a previous version of a certificate:

1. Open the certificate details page, and open **Previous Versions**.
2. Locate the version you want to revoke, and click **Revoke**.
3. In the Revoke window, click the **Reason for Revocation** list, and select the reason you are revoking this certificate.
4. [Optional] Provide a comment with additional information about the revocation reason.
5. Click **Revoke**.

Approve or reject a historical certificate revocation

If there is a workflow attached to the historical certificate revocation, an approver will need to authorize the action before it is actually revoked. The authorized approver will:

1. Open the All Certificates (dashboard), and click on the **Pending My Approvals** widget.
2. In the list of certificates requiring approval, use the Approve/Reject quick action.

3. Provide a comment on why you are approving or rejecting the certificate.
4. Click either **Reject** or **Approve**.

TIP You can also open the certificate's details page, and open Previous Versions, where you will see the Approve/Reject quick action button next to the historical certificate that is pending revocation.

Revert historical certificates

If you decide that you want to make a historical version the current version, you can revert to that version of the certificate. To do so, locate the certificate in the **Previous Versions** list, and click **Revert** in the action button. You can only revert valid certificates, so you cannot revert certificates that are expired or revoked.

Reverting a certificate means that what is now the current version will be moved to the previous versions list, and the version of the certificate that you select will become the new current version. You will be able to use this new current version for installation and monitoring purposes.

You can only see the **Revert** option in the action button if the following is true:

- You have the *Write* permission to the certificate.
- The certificate is not "In Error," "Expired," or "Revoked."
- The certificate is not in one of the following states:
 - installing
 - renewing
 - revoking of current
 - revoking of historical

WARNING! This action may cause the next renewal to be processed by the Certificate Authority as a new certificate, rather than as a renewal. For more information see ["How certificate renewal works"](#) on page 489.

IMPORTANT A private key that is associated with the certificate will only be restored if the certificate object is the owner of the private key vault.

Download historical certificates

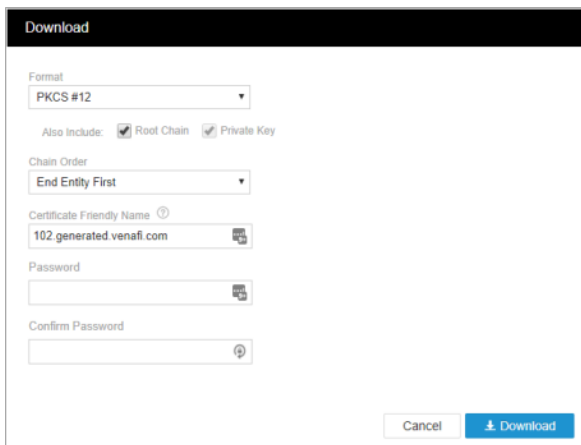
Historical certificates may still be valid, and you may want to download them for use.

If you need to download a historical version of the certificate to your local machine, use the following procedure:

1. Open the certificate details page, and open Previous Versions.
2. Locate the version that you want to download, and click **Download**.

NOTE If you can't see **Download** in the quick actions button, click the down arrow to show the additional actions.

3. In the Download window, select the download settings, and then click **Download**.

The screenshot shows a 'Download' modal window with a black header. The main area is white and contains several settings: 'Format' is set to 'PKCS #12' in a dropdown; 'Also Include' has checkboxes for 'Root Chain' and 'Private Key', both of which are checked; 'Chain Order' is set to 'End Entity First' in a dropdown; 'Certificate Friendly Name' is '102 generated venafi.com' with a help icon; 'Password' and 'Confirm Password' are empty text fields with icons to the right. At the bottom right are 'Cancel' and 'Download' buttons.

TIP If either the 'Root Chain' or 'Private Key' options are available on any of the keystore types, then the corresponding options will automatically be selected in the Download modal.

You will only be able to download the private key of a historical certificate if:

- You have the *Private Key Read* permission to the certificate.
- The certificate is an owner of the private key vault.

Managing Local Certificates Via Policy

Policies allow administrators to define global configuration parameters, or “folders,” for encryption resources associated with that policy, including local Certificate objects. For example, within a policy, you can standardize the key strength for all certificates created in that policy.

When a system object is defined under a policy object in the Policy Tree, the object and its corresponding resource are associated with the policy and are subject to the policy settings.

EXAMPLE If you configured the certificate management type in a Policy object, Trust Protection Platform would read those values for the policy’s subordinate Certificate objects. Thus, policies can be used to standardize object configuration parameters and enforce security requirements.

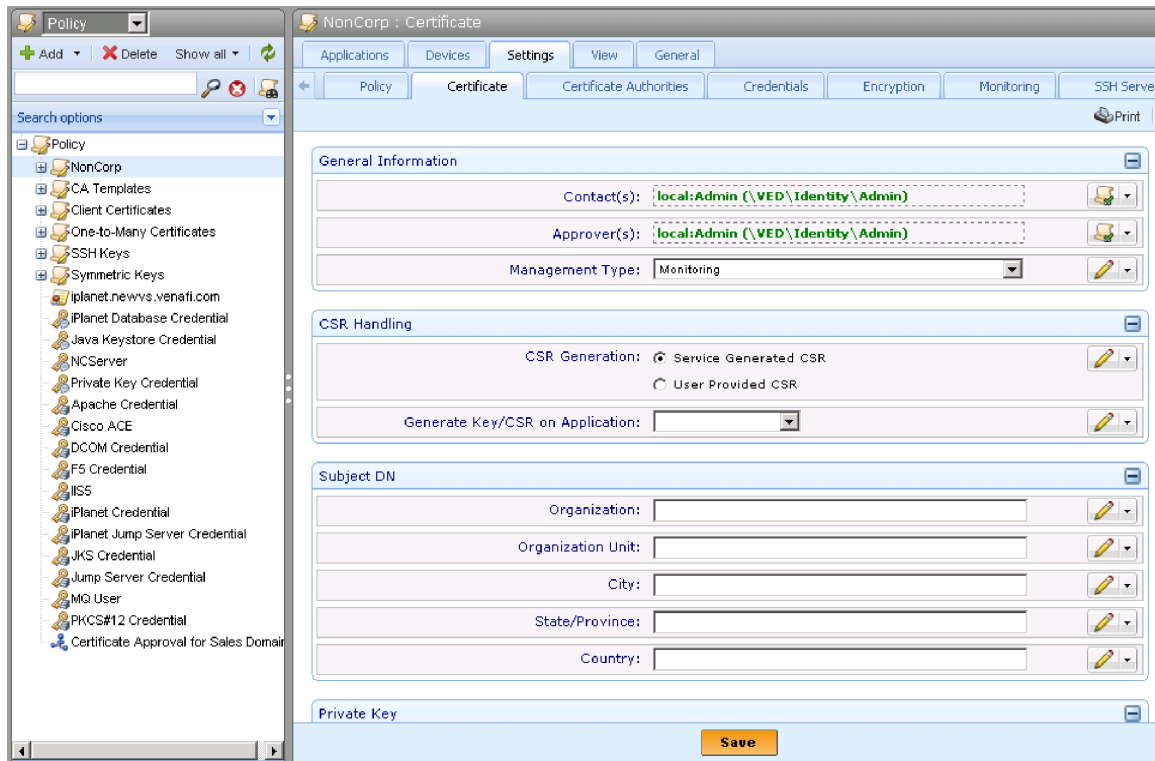
For more detailed information on how folders work, see [Using policies to manage encryption assets](#) in the Administration Guide.

You must have *View* and *Write* permissions on the object for which you want to configure settings.

To access the certificate settings in the Policy object

1. From the [TLS Protect menu bar](#), click Policy Tree
2. In the **Policy** tree, select the Policy object where you want to configure certificate settings, and then click the **Settings** tab.

The **Detail View** displays the Policy object’s associated settings.



There are two Policy configurations for Certificate objects: the Certificate and Monitoring tabs. The following sections outline these configuration options:

- "Policy object certificate settings" on the facing page
- "Policy object monitoring settings" on page 327

3. Define the settings you want to apply to the policy's subordinate Certificate objects.
4. Lock or unlock the value.

When you define an attribute within a Policy object, 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 .

To lock a policy value in Policy Tree

1. Click the **Unlocked** icon .

The value toggles between a locked  and unlocked  state.

2. When finished, click **Save/Apply**.

Policy object certificate settings

A policy object Certificate tab allows you to define settings, such as the certificate management type, for the subordinate certificate objects.

Certificate settings defined for a folder take precedence over the settings defined in the subordinate certificate objects *if* the values are locked. Otherwise, the policy's certificate settings function as default values for subordinate certificate objects.

The following table describes Policy Tree Policy object **Settings > Certificate** tab.

Field	Description
Certificate Tab	The Certificate tab defines certificate settings for subordinate certificate objects. Certificate settings defined at the folder level may take precedence over those defined in the subordinate Certificate objects. TIP The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the channel and notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393.
General Information	
Contacts	User or group identities assigned to subordinate certificate objects. Default system notifications are sent to the contact identities.

Field	Description
Approvers	User or group Identities assigned to approve workflows (certificate approval or injection command) for subordinate Certificate objects. For more information on defining Workflows, see "Implementing certificate workflow management" on page 557 . For information on when Trust Protection Platform references approvers defined in the Certificate object, see the option "Approver Assigned to Object" on page 571 .
Management Type	Level where subordinate certificates will be managed. The default is Provisioning. Trust Protection Platform provides the following levels of certificate management: ▪ Monitoring: Trust Protection Platform monitors existing certificates and provides current information on the certificate status and lifecycle. When the certificate nears the end of its lifecycle, Trust Protection Platform notifies the administrator. It does not, however, renew the certificate. The administrator must manually create the CSR, send it to the certificate authority (CA), then retrieve and install the renewed certificate. ▪ Enrollment: Trust Protection Platform can automatically generate and submit CSRs to Certificate Authorities using the parameters defined in designated CA Template objects. If preferred, the administrator can manually generate the CSR, then upload it to Trust Protection Platform to complete the enrollment process with the appropriate CA. After the CA signs the certificate, Trust Protection Platform retrieves the certificate and securely stores it in the central database. The administrator must then download the certificate from Trust Protection Platform and install it on the target systems. ▪ Provisioning: Trust Protection Platform manages the entire certificate lifecycle—it automatically requests, installs, and monitors your system 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.

Field	Description
Managed by	The Venafi application that manages the policy. Choose Aperture or User Portal if the policy is managed by that application. If not, leave this field blank.

CSR Handling

CSR Generation	Determines how CSRs are generated. The default is Service Generated CSR: ▪ Service Generated CSR: Trust Protection Platform automatically generates the CSR. ▪ User Provided CSR: CSR is manually generated by the administrator, then uploaded to Trust Protection Platform.

Generate
Key/CSR on
Application

Determines where the CSR and private key are generated. The default is No.

IMPORTANT When one or more of the following items are true, Remote Generation is *not* supported and, therefore, the *Generate Key/CSR on Application* setting is ignored.

- You're using a driver that does not support remote generation.
To learn which drivers support remote generation, see [Supported integrations: devices, applications, services and features supported by Venafi](#).
- You're using a self-signed CA template to enroll a certificate; self-signed CA templates do not work with remote generation.
This is because Trust Protection Platform requires that the private key be stored centrally so that it can be used to sign the self-signed certificate.
- Your certificate is associated with more than one application; to work correctly, the certificate must be associated with *one* application.
- You have not set the certificate's management type setting to Provisioning.
- You're doing one-to-many provisioning.

Field	Description
	If you do not select this option, the CSR and private key are centrally generated on the Trust Protection Platform server, then securely copied to the application. If you do select this option, the CSR and private key are locally generated on the application's server. In both cases, the certificate and private key are archived in the Trust Protection Platform database.
Hash Algorithm	For the certificate signing request, choose either SHA-256 , SHA-384 , or SHA-512 . The default is SHA-256.
Subject DN	
Organization	Name that uniquely identifies the organization in the certificate.
Organization Unit	Department or division within the organization that is responsible for maintaining the certificate.
City, State/Province, Country	Location (city, state/province, and country) of your Organization or Organizational Unit.
Domain White List	
Allowed Domains	Enter the suffix of allowed domains. For example, <i>.com</i> <i>acme.com</i>, or <i>sales.acme.com</i>. If you leave this field blank, all domains will be allowed.
Allow Wildcards	The default is Yes . Select No to prohibit wildcards.
Allow Duplicate Common and Subject Alternate Names	The default is Yes . Select No to require unique names.

Field	Description
Private Key	
Reuse Private Key for Service Generated CSRs	Reuses the original private key when renewing the certificate. The default is No.
Allow Users to Import Duplicate Certificates and Reuse Private Keys	Controls the reuse of certificates and private keys. When enabled, this permits you to import a certificate even if another certificate with the same private key already exists in the system. It would also allow you to renew a certificate without uploading / re-generating a new private key. When disabled, if you are renewing a certificate with a user-provided CSR, you cannot reuse a CSR that is tied to a private key that has ever been uploaded to Trust Protection Platform. Also, when importing a certificate manually, through WebSDK and Web UI, you won't be able to upload a certificate that is already in the inventory. We recommend you leave this option disabled (unchecked). NOTE If you enable this option, you must have Write permission for the original certificate. Failing to have this permission will result in the system producing an error message: <code>Duplicate Certificate. Insufficient Permissions to View Existing Certificate.</code>
Allowed Algorithms	Dictates which algorithms can be used within the scope of the policy. Administrators can use the controls in the UI to add and remove allowed algorithms. To see a list of supported algorithm types, see Algorithm types supported by Venafi Platform. To learn more about algorithms, see Understanding cryptographic algorithms in Venafi Trust Protection Platform.
Default Algorithm	Sets an algorithm (chosen from the allowed list) to use when a certificate doesn't specify one. Administrators can use the controls in the UI to make sure that a default is always in place.

Field	Description
	The Use System Default option means to use whatever algorithm is currently selected as the default for that policy. This setting has its own policy control, which can be set on a per-policy basis. If none are set, it falls back to the global default list configured in VCC.s
Other Information	
CA Template	CA Template object that reTrust Protection Platformferences to generate the CSR and submit it to the CA.
Key Generation	Encryption key to generate the certificate private key. By default, Trust Protection Platform provides an AES-256 encryption key—the Venafi Platform software key—to generate private keys. However, you can also configure Trust Protection Platform to use AES encryption keys stored on supported HSM devices to generate certificate private keys. Your system is protected by either a hardware or a software encryption key (or both).
Encryption Key	Encryption key to use to protect the certificate private key. The system uses either a hardware or software key (or both). The software encryption key secures data in the Trust Protection Platform database, and is stored in the Windows registry. You can also configure Trust Protection Platform to use AES encryption keys stored on supported HSM devices to encrypt your system certificates. For information, see Managing system encryption keys in the <i>Trust Protection Platform Administration Guide</i>.
Disable Automatic Renewal:	Disables enrollment and provisioning for the current certificate. This means that Venafi TLS Protect does not attempt to renew or install the current certificate. However, Venafi TLS Protect still provides monitoring, validation, and notification for the certificate object. Additionally, the certificate is represented in Dashboard statistics and system reports. The default is No.

Field	Description
	Trust Protection Platform automatically selects this option when it renews a certificate in response to a SCEP request.
Allow Simple Passwords for Private Key Downloads	The setting to control whether simple or strong passwords are required for private key downloads. The default is No.
PKCS#12 Encryption Algorithm	Each algorithm has its own security and compatibility level. Generally, higher security means lower compatibility with software applications.
Private Key PBE (password-based encryption) algorithm	This setting applies to private keys that are downloaded using the PEM format. Options include: Insecure but good system compatibility, Insecure but better system compatibility (SHA1 3DES), High security but low system compatibility (SHA256 AES256). The default is <i>High security but low system compatibility (SHA256 AES256)</i>. You should not change it unless you have an incompatible system that cannot be upgraded. For more information, see "Using PBE (password-based encryption) algorithms to secure private keys" on page 329. NOTE The algorithms used to derive the protection key and encrypt the private key are not supported by all applications. Generally, the more secure the protection key and algorithm, the fewer applications will support it.
Renewal Window	Number of days prior to expiration that Trust Protection Platform begins the renewal operation. The default and recommended value is 30 days.

Field	Description
Validation	The purpose of Network Validation is to confirm that the certificate is functional and to verify that the correct certificate is being used. Network Validation requires network access to the server where the application is installed.
Disable SSL/TLS Validation	Disables Network Validation, including all related notifications, for subordinate Certificate objects.
Network Port	Port that the Validation Manager uses to connect to the server where the application is installed. The Validation Manager uses an SSL connection to validate the application's associated certificate. The default port is 443.
Use certificate's Common Name	Require validation scans to use a DNS lookup to resolve the certificate Common Name. Validation occurs on the certificate at every IP address returned from the DNS lookup. The default is Yes.
Use certificate's DNS Subject Alternative Names	Require validation scans to validate DNS Subject Alternative Names (SANs) of the certificate, if any. The default is No.
Validate the chain returned by the hosting server	Validate the chain returned by the hosting server to the chain that Trust Protection Platform builds using its internal algorithm to ensure a match. The default is yes, meaning chain validation is enabled and it affects the SSL/TLS validation result.
Approved Certificate Authorities	Available only in the Root Policy object.
Approved for Issuance	Available only in the Root Policy object. Select certificate authorities (CAs) you want to be considered trusted and approved issuers. This list is useful in identifying certificates issued by unapproved CAs. You can configure the Critical Alerts widget in the product dashboard to identify certificates that do not match your approved CA list.

Field	Description
Active Directory Certificate Authentication	Device, user, server, and certificates policy settings related to Active Directory certification authentication and SID (security identifier).
Allow certificates with AD Security Identifier (SID)	The default is No. If set to No, Trust Protection Platform will not allow certificates with an SID extension.
Allow security identifiers outside of connected identities	The default is No. Controls whether Trust Protection Platform allows unknown SID (security identifier). If set to No and Trust Protection Platform cannot find the provided SID value in AD, the certificate request is rejected.
Automatically include requester identity	The default is Yes. Applies to WebSDK. If set to Yes, the WebSDK requester identity is set as the AD security identifier (SID) identity, unless provided with the request. If Trust Protection Platform cannot resolve objectSid from the WebSDK requester identity, it is ignored. If the resolved SID value doesn't match the policy settings, then the request is rejected.
AD Security Identifier source	Choose between: - Look up SID from AD Identity. Resolves SID from the provided AD identity. - Enter SID manually. Manually-specified SID. Supports macros. Main use case for macros is to set a setting on a policy and lock it. If a macro is provided with the request, the Allow security identifiers outside of connected identities setting must be set to Yes.

Policy object monitoring settings

The policy object's Monitoring page allows you to define the intervals at which Trust Protection Platform generates expiration events for the Policy object's subordinate Certificate objects.

The following table describes the options in the Policy Object's **Settings > Monitoring** tab:

Field	Description
Monitoring Tab	The Monitoring tab defines the expiration event settings for subordinate objects—you can define how soon and how often expiration events are generated for the policy's subordinate Certificate objects. Monitoring parameters defined in folder may take precedence over the monitoring parameters defined in the Certificate objects. The recipients and delivery method (email, SNMP trap, etc.) for expiration notifications are defined in Notification and Channel objects. You must configure the Channel and Notification objects to send notifications for expiration events. For more information, see "Managing certificate notifications" on page 393 in the Certificate Management guide.
Expiration Start	Number of days before a certificate expires that you want to start generating expiration events.
Expiration Interval	Frequency (in days) at which you want Trust Protection Platform to generate expiration events.
Escalation Start	Number of days before a certificate expires that you want to start generating escalated expiration events.

Field	Description
Escalation Interval	Frequency (in days) at which you want Trust Protection Platform to generate escalated expiration events.
Disabled	Disables Monitoring for all subordinate Certificate objects.
Policy	Allows you to lock a value within the Policy object. Locked attributes cannot be modified in subordinate Certificate objects. Unlocked attributes function as suggested values; they can be accepted or overwritten in the subordinate object configuration. By default, policy values are unlocked . The value toggles between a locked  and unlocked  state. The first Policy icon locks or unlocks the Expiration Start values. The second Policy icon locks or unlocks the Escalation Start values. The third Policy icon locks or unlocks the Disabled value.

Using PBE (password-based encryption) algorithms to secure private keys

To help secure private keys in your environment, Venafi requires that all private keys that are downloaded are password encrypted. Trust Protection Platform lets you use *password-based encryption* (PBE) algorithms to secure all PKCS#8-formatted private keys that are downloaded from Aperture, Policy Tree, or WebSDK.

TIP When selecting one of the supported PBE options, keep in mind that the relationship between *security* and *compatibility* is inverse: the higher the security, the lower the system compatibility, and vice versa.

NOTE Because OpenSSL supports only MD5 for key derivation, it is a legacy private key format that is very compatible but is insecure and the NIST considers it to be retired. For better security, you can disallow this format by locking the PBE algorithm policy to Medium or High. For best security, we recommend you lock the PBE algorithm policy to High for all certificates.

When configuring PBE, you select one of the following options:

PBE options (algorithms)	Hashing algorithm	Cipher used to encrypt/decrypt
Insecure but good system compatibility	MD5	DES
Deprecated but better system compatibility	SHA1	3DES
High security and compatible with newer application versions (system default)	SHA256	AES256

To configure this setting in Policy Tree

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. Click the appropriate policy.
3. Click the **Certificate** tab.
4. In the **Other Information** area, click the **Private Key PBE Algorithm** arrow.
5. Choose the algorithm that best fits your needs.

To learn how to configure this setting in TLS Protect's modern interface, see ["Setting policy on a folder" on page 177](#).

Determining certificate compliance

The **Compliance** tab provides an assessment of the certificate's compliance with its parent folder.

- The Certificate Value column lists the certificate values as they are currently defined in the certificate. Certificate Values are listed as being in  or out  of policy.
- The Renewal Value column lists the certificate values currently defined in the Certificate object. Renewal values also reflect policy status.

cert : Compliance

Certificate Monitoring Validation General

Summary Settings Associations Compliance History

Print

Subject DN & Key Strength

	CERTIFICATE VALUE	RENEWAL VALUE
Common Name:	cert	cert
Subject Alt Name (DNS):		
Organization:		
Organization Unit:		
City:		
State:	Utah	Utah
Country:	US	US
Key Strength (bits):	1024	

Other Information

Certificate Authority:	VenQA CA
Public Key Algorithm:	rsaEncryption
Signature Algorithm:	sha1RSA

7

Managing root certificates

When the Server Agent scans local file systems and keystores, it discovers all X.509 certificates, including root and intermediate root certificates.

After you discover the root and intermediate root certificates deployed on local systems, you can bring those certificates under management for monitoring. You can also download and share the root and intermediate root certificates with other systems.

Additionally, Trust Protection Platform allows you to manually upload root and intermediate root certificates, which can also be monitored and shared.

This chapter contains the following topics:

Bringing discovered root certificates under management	334
Manually adding root and intermediate root certificates	334
Deleting Root or Intermediate Root Certificates	336
Downloading root chains	336
Blacklisting root or intermediate root certificates from chain building	338

Bringing discovered root certificates under management

Trust Protection Platform allows you to bring root and intermediate root certificates discovered during Agent Discovery under management from the Discovery Results tabs of your Certificate Module Discovery object.

NOTE By default, when the Trust Protection Platform agents upload their scan results to the KMIP server, Trust Protection Platform does not exclude root certificates that are currently under management. If you want to exclude currently managed root and intermediate root certificates from the Certificate Module Discovery results, you can define an Exclusion object, then reference that Exclusion object in the Certificate Module Discovery object. For more information on this procedure, see .

Agent Discovery is the fastest and easiest way to bring root and intermediate root certificates under management because the Discovery feature automatically imports the certificate.

Manually adding root and intermediate root certificates

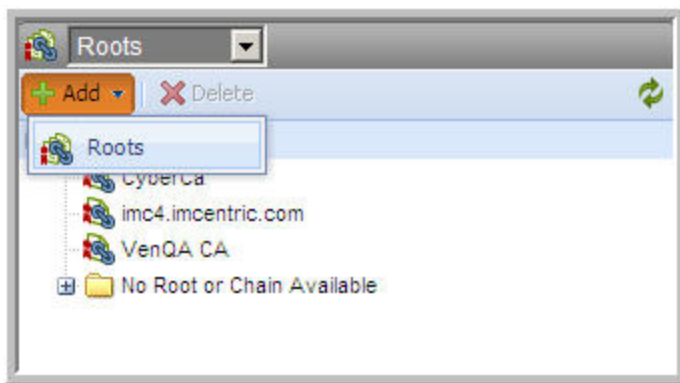
The Server Agent trust bundle is built automatically. However, if you need to import or re-import the root and intermediate root certificates, you can do so manually by following the procedure in this topic.

Before you can manually import a root or intermediate certificate, you must have *write* permissions and *create* permissions to the Roots object in the Roots tree. Once you have the correct permissions, then complete the following procedure.

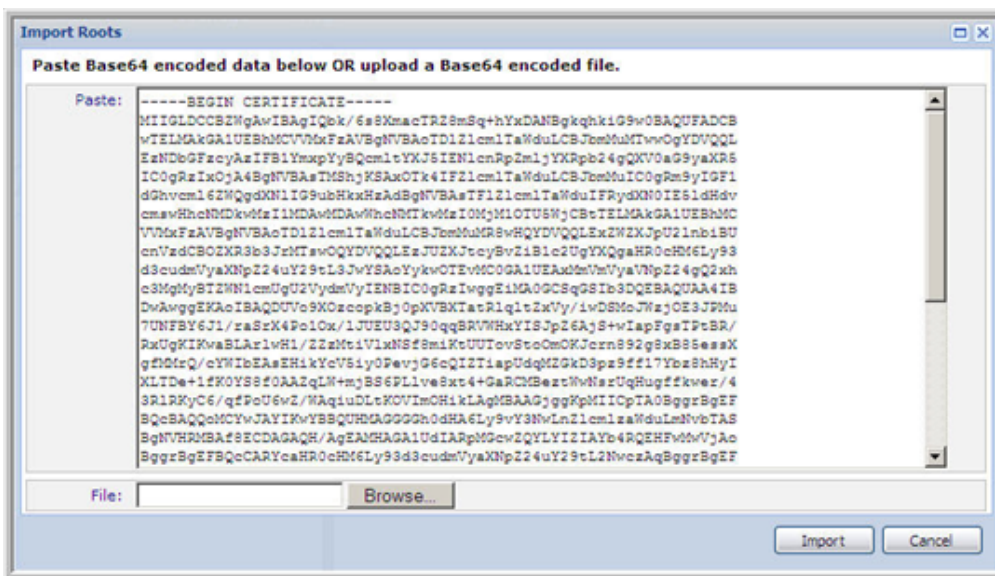
NOTE During this procedure, you must also have access to the certificates so that you can copy their source into the **Import Roots** dialog.

To import a root or intermediate root certificate to the Trust Protection Platform database

1. From the **TLS Protect menu bar**, click **Policy Tree**.
2. Select the **Roots** tree from the **Tree** drop-down menu.
3. In the **Roots** tree, click **Add > Roots**.



The Import Roots dialog appears.



4. Do one of the following:
 - a. Copy and paste the Base64-encoded root or intermediate root certificate source from the certificate file into the **Paste** field.

You must copy the entire certificate source, including the Begin Cert and End Cert text.
 - b. Click **Browse** to select a Base64-encoded file from the file system.
5. Click **Import** to import the root or intermediate root file into the Trust Protection Platform database.

Look in the **Roots** tree for your new root or intermediate root certificate.

Deleting Root or Intermediate Root Certificates

You must have *delete* permissions to the Root Certificate object to delete a root or intermediate root certificate. Once you have established permissions, complete the following procedure.

To delete a root or intermediate root certificate

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. Select the **Roots** tree from the Tree drop-down menu.
3. In the Roots tree, select the root or intermediate root certificate you want to delete, and then click **Delete**.
4. Click **Yes** to confirm.

Downloading root chains

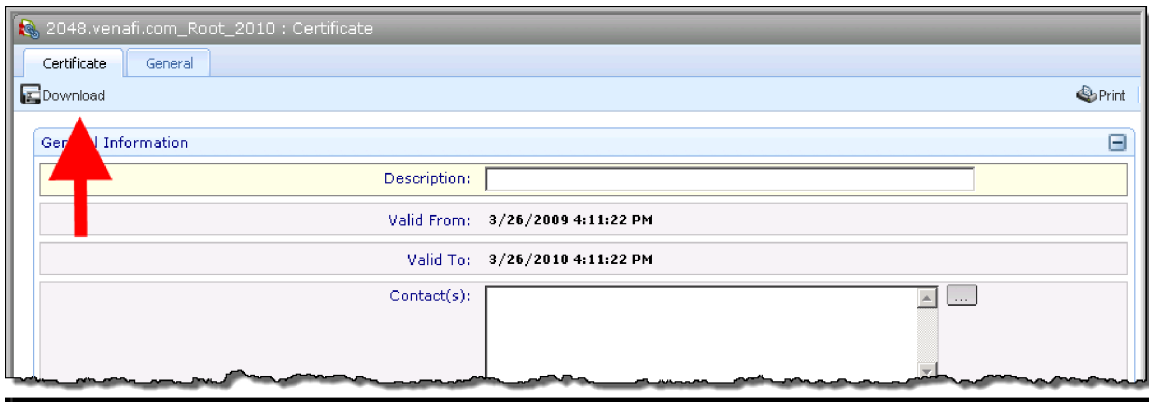
You can download the root chain from the Trust Protection Platform database so you can manually install them on your servers.

You must have *View* and *Write* permissions on the object for which you want to configure settings.

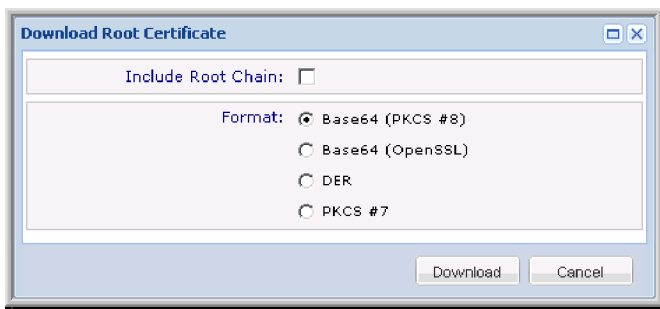
This option is available only in Policy Tree.

To manually download a root chain

1. From the [Platform menu bar](#), click Policy Tree.
2. Select the **Roots** tree from the Tree drop-down menu.
3. In the Roots tree, select the Root Certificate object from which you want to download the root chain.
4. Click the **Certificate** tab.
5. Click **Download**.



6. The Download Certificate dialog appears.



7. Designate the format in which you want to save the certificate files.

- Base64 (PKCS#8)
- Base64 (OpenSSL)
- DER
- PKCS#7

8. Click **Download**.

9. In the **File Download** dialog, click **Save**, and then browse to the Directory where you want to save the file.

10. Click **Save**.

You can now use the downloaded file to install the root chain on other systems.

Blacklisting root or intermediate root certificates from chain building

When there are problems with incorrect chains being used with provisioning or downloading, the problem root certificate can be removed from future chains by simply marking it as **blacklisted everywhere** in the Roots tree.

If the certificate is not already in the Roots tree, upload it or move it to the Roots tree first.

For more information, see "[Managing root certificate trust](#)" on page 340 in the *Venafi Trust Protection Platform Installation Guide*.

8

Managing certificate trust

Trust Protection Platform helps you secure and protect your network by letting you *whitelist* and *blacklist* certificates. You can then bundle them together—called a *trust bundle*—and then put those bundles into a trust store. The trust store can then be installed on one or more devices and managed using the Policy tree.

Using trust bundles means that you no longer have to track and manage individual certificates in your trust stores. You can create bundles of trusted certificates and then deploy them to devices via trust stores.

This chapter contains the following topics:

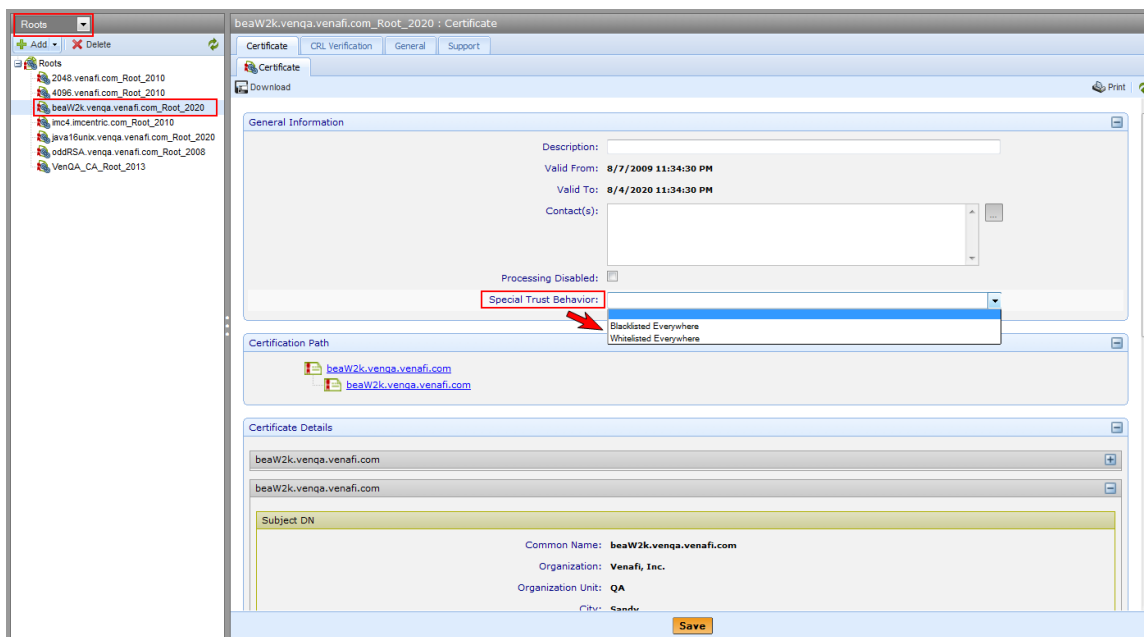
Managing root certificate trust	340
Managing certificate bundle objects	341
Creating and managing trust stores	348
Adding a trust bundle to a trust store	377
Provisioning bundles to trust stores	383
About Domain Whitelisting	391

Managing root certificate trust

Root and intermediate certificates can easily be whitelisted and blacklisted directly from the Roots tree.

To whitelist and blacklist root certificates

1. In the **Roots** tree, and then click the root certificate that you want to work with.
2. On the **Certificate** tab, in the **General Information** group box, click the **Special Trust Behavior** drop-down arrow.



There are three choices:

- **Blank** – This is the default setting. The certificate is neither whitelisted nor blacklisted.
- **Whitelisted Everywhere** – The root certificate is always trusted and accepted. When a Trust Store that Trust Protection Platform is managing is provisioned, the certificate will be added to the Trust Store.
- **Blacklisted Everywhere** – The root certificate is never trusted or accepted. When a Trust Store that Trust Protection Platform is managing is provisioned, the certificate will be removed from the Trust Store.

3. When you're done, click **Save**.
4. (Optional) Review these certificates in an Effective Bundle from any Trust Store object. To learn more, see ["Viewing the Effective Bundle" on page 346](#)

Managing certificate bundle objects

Trust Protection Platform helps you secure and protect your network by letting you *whitelist* and *blacklist* certificates. You can then bundle them together—called a *trust bundle*—and then put those bundles into a trust store. The trust store can then be installed on one or more devices and managed using the Policy tree.

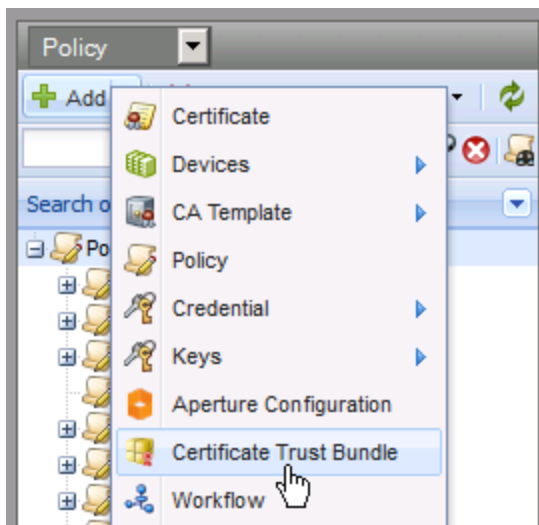
The topics in this section show you how to create and manage trust bundles.

Creating a certificate trust bundle

You can create a bundle of trusted certificates by whitelisting or blacklisting them. The bundle can then be assigned to trust stores.

To create a certificate trust bundle

1. In the **Policy** tree, click **Add > Certificate Trust Bundle**.



2. In the **General** box, type a name for your new trust bundle.

(Optional) Type a description of the purpose of your trust bundle that can help you identify its purpose later on.

3. In the **Certificates** box, do one of the following:
 - Click the Add buttons to select certificates to include in either the whitelist and blacklist boxes.
 - (Optional) To make a faster selection, select only whitelisted certificates and then enable **Blacklist all other certificates** to let Trust Protection Platform blacklist remaining certificates.

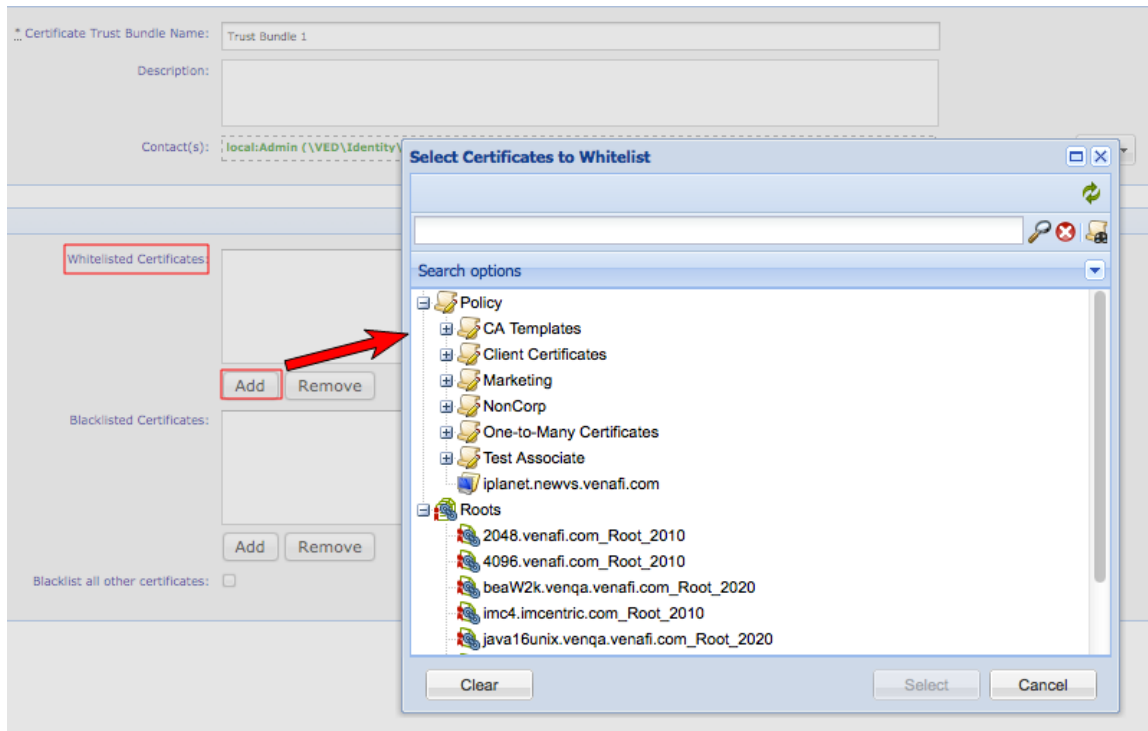
4. When you're finished, click **Save**.

Strict matches versus allowable matches

You can make certificate matches in bundles strict or loose depending on how you whitelist and blacklist certificates.

To create a strict match for a trust bundle

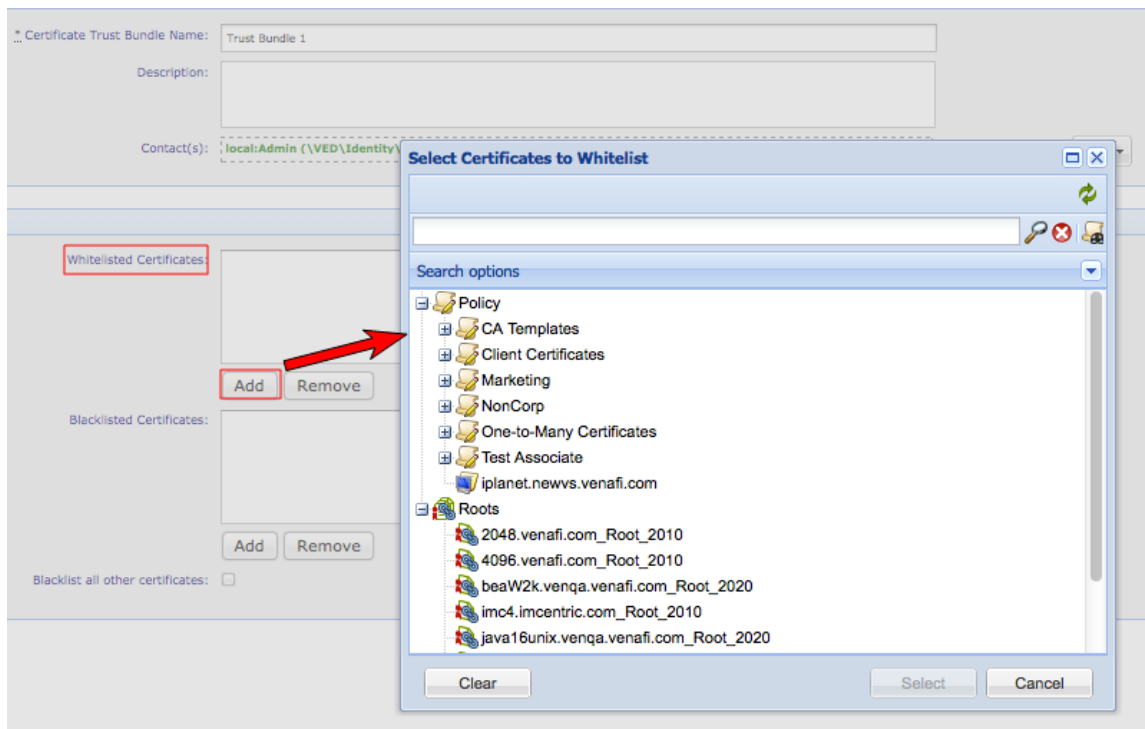
1. In the **Select Certificates to Whitelist** box, **Add** the certificates that are always trusted and accepted.



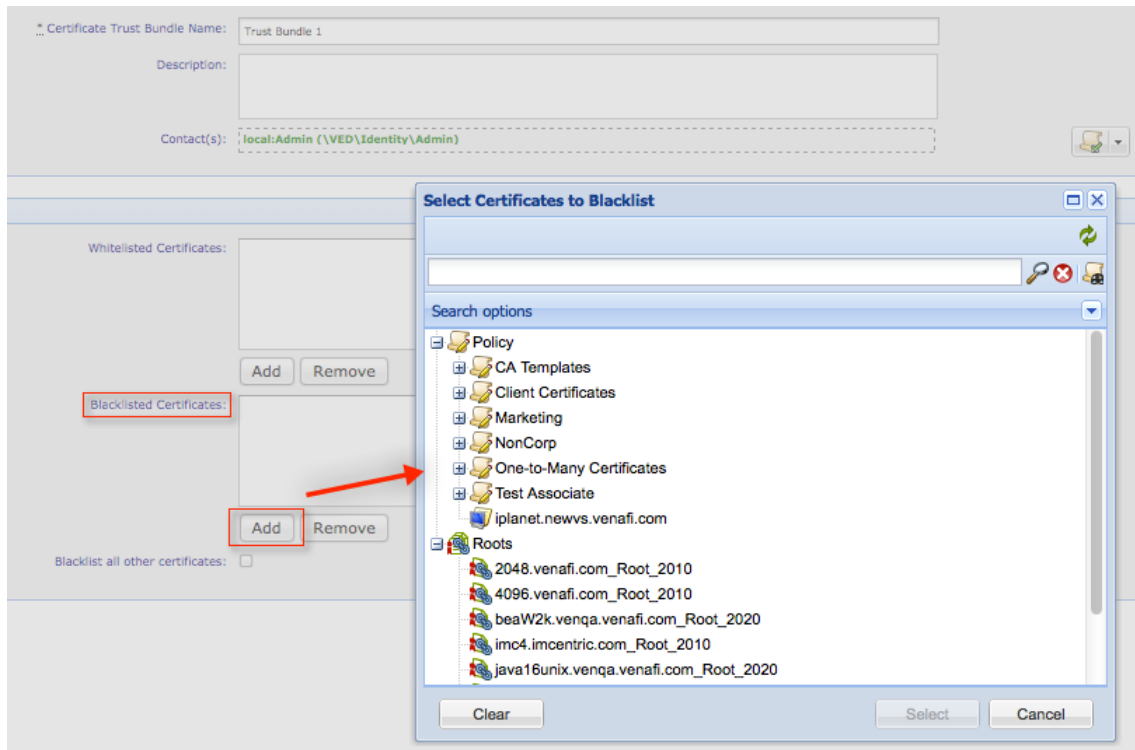
2. In the **Select Certificates to Blacklist** box, select **Blacklist all other certificates**.
3. When you click **Save**, you'll have created a *strict match* trust bundle because you have explicitly specified the certificates that are trusted and untrusted.

Create an allowable match for a trust bundle

1. In the **Select Certificates to Whitelist** box, **Add** the certificates that are always trusted and accepted.



2. In the **Select Certificates to Blacklist** box, **Add** the certificates that are never trusted and accepted.



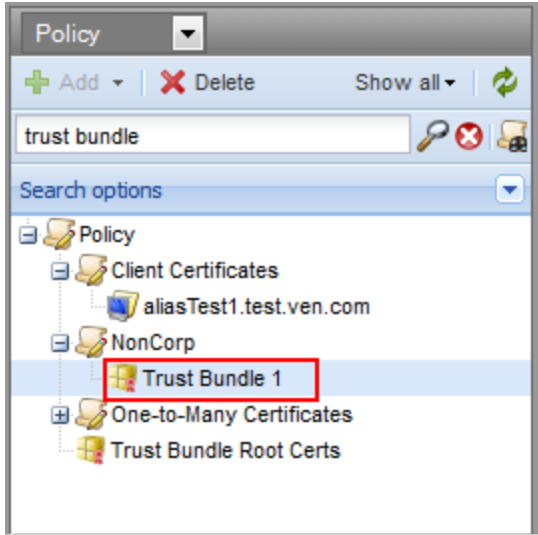
3. When you click **Save**, you'll have created a *allowable match* trust bundle because you have specified which certificates are trusted and which are untrusted but you haven't excluded other certificates.

Viewing trust bundle associations

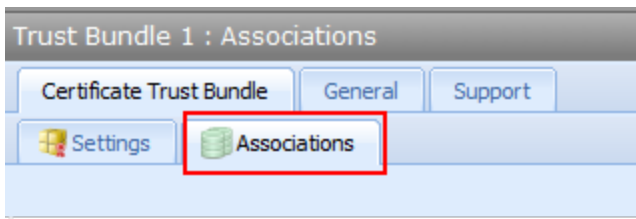
You can see which targets a bundle is associated with so that you can understand the impact the bundle will have on trust stores.

View a trust bundle association

1. In the **Policy** tree, click the trust bundle for which you want to see associations.



2. Click the **Associations** tab.



3. In a view-only grid, the DN, Object Type, Status, and Last Provisioned are displayed for each location in which the trust bundle is found..

The screenshot shows the 'Trust Bundle 1 : Associations' view. The table displays the following data:

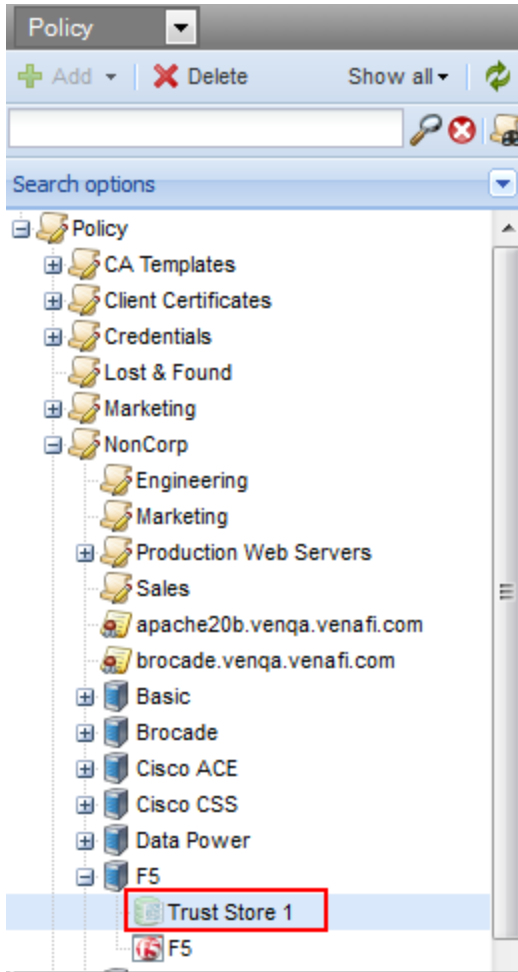
DN	Object Type	Status	Last Provisioned
\\VED\\Policy\\NonCorp\\FS\\Trust Store 1	PEM Trust Store	OK	
\\VED\\Policy\\NonCorp\\PEM\\JKS Trust Store	JKS Trust Store	OK	

Viewing the Effective Bundle

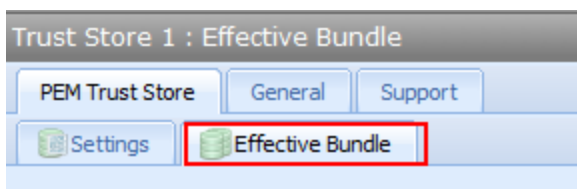
The Effective Bundle gives you detail about the trusted and untrusted certificates and bundles in a particular trust store.

To view a trust store's effective bundle

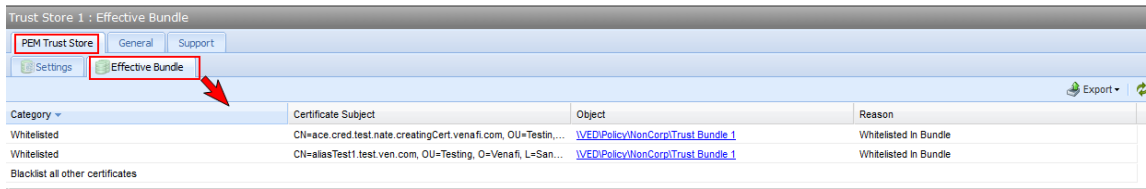
1. In the **Policy** tree, locate the trust store whose effective bundle you want to view.



2. Click the **Effective Bundle** tab.



3. A view-only grid shows you details of all of the certificates in the effective bundle for the trust store.



4. Click a blue link to view or edit a trust bundle.

Creating and managing trust stores

A *trust store* is a collection of root certificates that are trusted by default and are maintained by the companies that make operating systems and web browsers, such as Apple, Microsoft, Mozilla, and Google. Each has its own standards and requirements for root certificates but they all require an issuing CA to undergo one or more audits before their root certificate is included.

You can configure trust stores—including certificate trust bundle assignments, using a policy, which is the recommended method when you have many trust stores with the same configuration.

Trust Protection Platform lets you create the following types of trust stores:

- Blue Coat SSLVA Trust Store
- CAPI Trust Store
- Connect:Direct Trust Store
- F5 LTM Advanced Trust Store
- GSK Trust Store
- IBM DataPower Trust Store
- JKS Trust Store
- Palo Alto Networks FW Trust Store
- PEM Trust Store
- PKCS#12 Trust Store

This section explains how to create trust stores. These trust stores can then be added to devices and if you want, provisioned automatically.

This chapter contains the following topics:

About creating and configuring trust stores

Because certificate trust stores contain trust bundles, it's a good idea to create your certificate trust bundles first. Then you can create and configure a trust store and assign one or more of those bundles to it.

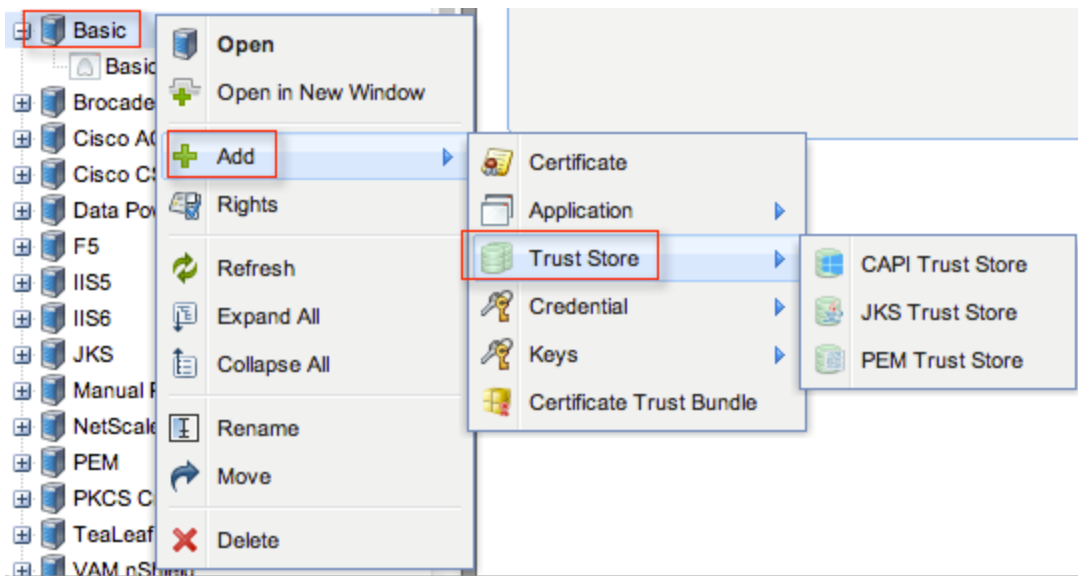
Certificate trust bundles can be assigned to all trust stores of the same type (e.g., PEM, CAPI, or JKS). Anytime you install a trust store of a particular type on a device, all of the whitelisted and blacklisted certificates are already specified.

If you're not quite sure how to create trust bundles, see ["Creating a certificate trust bundle" on page 341](#).

After you've created device objects, then you simply select your device and add and configure one or more trust stores. You can assign an unlimited number of trust stores to a single device and the trust stores can be of the same type (e.g. PEM, JKS, and CAPI).

Regardless of the type of trust store you create, the steps to create a trust store are mostly the same; however, each trust store type includes some unique settings.

1. In the **Policy** tree, right-click a device.
2. Click **Add > Trust Store**, and then select the type of trust store you want to add.



3. Under **General**, in the **Certificate Trust Store Namebox**, type a name for your new trust store, and then add an optional description.

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.

4. If the policy that governs this device allows it, add the appropriate certificate trust bundles.

Add New : CAPI Trust Store

Status

Status: **Ok (Processing Disabled)**

Processing Stage: **none**

Last Provisioned: **never**

Processing Disabled: ☒

General

* Certificate Trust Store Name:

Description:

Contact(s):

Approver(s):

Certificates Trust Bundles

Certificate Trust Bundles:

Provisioning Interval

Disable scheduled provisioning:

Provision every: days

Application Information

Application Credential:

Connection Method: **WinRM**

Port:

Save

This chapter contains the following topics:

Configuring a Blue Coat trust store

You can configure a trust store by creating trust bundles and assigning one or more of those bundles to the trust store. The trust store can then be installed on one or more devices. For more information, see "Creating a certificate trust bundle" on page 341.

To configure a Blue Coat trust store

1. From the **TLS Protect menu bar**, click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > Blue Coat Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.

	Settings	Description
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.

Settings		Description
Trust Store Settings		
Blue Coat	Create Lists	If this setting is set to Yes, when a specified list name does not exist, it will be created so that the certificate being provisioned can be added to it.
	Trusted Certificates List	Enter the names of one or more lists to which the certificate will be added in addition to the all-trusted-certificates list..

4. When you're finished, click **Save**.

Configuring a CAPI trust store

You can configure a trust store by "[Creating a certificate trust bundle](#)" on [page 341](#) and assigning one or more of those bundles to the trust store. The trust store can then be installed on one or more devices.

To configure a CAPI trust store

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > CAPI Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.

	Settings	Description
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
CAPI	Log Windows Events	Select Yes or No to enable log events.

- When you're finished, click **Save**.

Configuring an IBM DataPower trust store

By taking a few steps in Trust Protection Platform, you can provision certificate trust bundles to your IBM DataPower appliances.

This topic shows you how to create and configure an IBM DataPower trust store object on the associated DataPower device object with the certificate trust bundles you want provisioned to your IBM DataPower appliance.

TIP Make sure that you've already created the certificate trust bundles you want provisioned to DataPower. You'll need to select them during the following procedure. If you're not sure how, see "Creating a certificate trust bundle" on page 341.

To configure a IBM DataPower trust store

1. From the **TLS Protect menu bar**, click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > IBM DataPower Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
General	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store.
		DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
	Certificate Trust Store Name	Enter the name of the Certificate trust store.

	Settings	Description
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
IBM DataPower	Certificate Bundle Folder	(Required) Select where the certificates will be stored. The default value is <i>cert</i> .

Settings	Description
Crypto Validation Credential Name	(Required) Type the name of the Crypto Validation Credential to which all certificates from the bundle are to be assigned.
Application Domain	Type the domain where the certificate and private key are installed on the DataPower device. If left blank, provisioning is done to the default DataPower domain.
Certificate Validation Mode	(Required) Select which method should be used to perform the certificate validation. <i>Match exact certificate or immediate issuer</i> is the default value.
Use CRL	Select whether to use CRLs during validation. The default value is <i>Yes</i> .
Require CRL	Select whether to require CRLs during validation. The default value is <i>No</i> . This option is only available if Use CRL is set to <i>No</i> .
CRL Distribution Points Handling	Select how Distribution Point certificate extensions should be handled by setting to either <i>Ignore</i> (default setting) or <i>Require</i> . This option is only available if Use CRL is set to <i>No</i> .
Check Dates	Select whether dates should be checked during certificate validation. The default value is <i>Yes</i> .

- When you're finished, click **Save**.

Configuring an IBM Sterling Connect:Direct trust store

This object represents a trust store in Connect:Direct format, which is a binary file that contains certificates and can be managed from the command line using the Java keytool utility. The default Java trust store file is named *cacerts*.

To configure a Connect:Direct trust store

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > Connect:Direct Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store.

	Settings	Description
		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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.

Settings		Description
Trust Store Settings		
Connect:Direct	Node Name	The name of the Connect:Direct Secure+ node. Trust Protection Platform provisions the certificate and private key to this node.
	Trust Store Label	Enter a label for this Trust Store.

4. When you're finished, click **Save**.

Configuring an F5 LTM Advanced trust store

This object represents a trust store in F5 LTM format, which is a text file that contains Base64 certificates.

To configure a F5 LTM Advanced trust store

1. From the **TLS Protect menu bar**, click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > F5 LTM Advanced Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

Settings		Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the

	Settings	Description
		certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.

	Settings	Description
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
F5 LTM Advanced	Certificate Bundle Name	Enter a name for the certificate bundle. To learn more about bundles, see "Managing certificate bundle objects" on page 341 .

4. When you're finished, click **Save**.

Configuring a GSK trust store

You can configure a trust store by ["Creating a certificate trust bundle" on page 341](#) and assigning one or more of those bundles to the trust store. The trust store can then be installed on one or more devices.

To configure a GSK trust store

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > GSK Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.

	Settings	Description
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
GSK	Trust Store Path	Specify the path to the file that is being Provisioned.

Settings	Description
Trust Store Credential	A password is required in order to add or remove certificates from the keystore. In the Credential Selector list, choose the appropriate stored credential.
Use FIPS	Creates the keystore and manages certificates and private keys in accordance with the Federal Information Processing Standard (FIPS). Version 4 CMS keystores are considered FIPS compliant whereas Version 3 CMS keystores are not. If the keystore to which certificates are to be provisioned already exists, this setting must be consistent with the settings used when it was created.
Stash Password	Generates an .sth file that stores the keystore password. Servers and applications reference the .sth file to obtain keystore passwords.

4. When you're finished, click **Save**.

Configuring a JKS trust store

This object represents a trust store in JKS format, which is a binary file that contains certificates and can be managed from the command line using the Java keytool utility. The default Java trust store file is named *cacerts*.

To configure a JKS trust store

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > JKS Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.

	Settings	Description
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
JKS	Trust Store Type	Choose either JKS or JCEKS. JKS is the standard open format. Choose JCEKS only if your application specifically requires it.
	Trust Store Path	Specify the path to the file that is being Provisioned.
	Trust Store Credential	A password is required in order to add or remove certificates from the keystore. In the Credential Selector list, choose the appropriate stored credential.

- When you're finished, click **Save**.

Configuring a Palo Alto Networks trust store

You can configure a trust store by creating trust bundles and assigning one or more of those bundles to the trust store. The trust store can then be installed on one or more devices.

To learn more, see ["Creating a certificate trust bundle" on page 341](#).

To configure a Palo Alto Networks FW trust store

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > Palo Alto Networks FW Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store.

	Settings	Description
		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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341 .
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.

Settings		Description
Port		Specify the associated port number for the Connection Method.
Trust Store Settings		
Palo Alto Networks	Lock Config	This setting controls whether Trust Protection Platform should lock the Palo Alto Networks Firewall configuration while it is actively provisioning the certificate. Locking the configuration prevents the driver from committing changes that it did not make. If the configuration is not locked, the driver may commit any changes that were already pending on the firewall at the time of provisioning.

4. When you're finished, click **Save**.

Configuring a PEM trust store

This object represents a trust store in PEM format, which is a text file that contains Base64 certificates.

To configure a PEM trust store

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > PEM Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store. DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store. 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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.

	Settings	Description
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
	Provisioning Interval	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.
Trust Store Settings		
PEM	Trust Store Path	Specify the path to the file that is being Provisioned.

- When you're finished, click **Save**.

Configuring a PKCS#12 trust store

You can configure a trust store by creating trust bundles and assigning one or more of those bundles to the trust store. For more information, see ["Creating a certificate trust bundle"](#) on page 341

The trust store can then be installed on one or more devices.

To configure a PKCS#12 trust store

1. From the [TLS Protect menu bar](#), click **Policy Tree**.
2. From the Policy tree, locate and right-click your device object, and then click **Add > Trust Store > PKCS#12 Trust Store**.
3. On the **Settings** tab of the new trust store object, refer to the following table to configure the new trust store:

Trust Store Object Settings

	Settings	Description
Status	Status	Current status of the trust store
	Processing Stage	If the Application's certificate is currently under processing, Trust Protection Platform indicates the current stage of the certificate lifecycle
	Last Provisioned	Date that the trust store was most recently provisioned.
	Processing Disabled	If the checkbox is selected, trust store processing is currently disabled. Clear this checkbox to enable the trust store.
	DID YOU KNOW? When disabled, you can save the new trust store object without completing all of the required fields. When enabled, you must fill in all required fields before you'll be allowed to save your changes.	
General	Certificate Trust Store Name	Enter the name of the Certificate trust store.
	Description	Enter an optional description of the trust store.

	Settings	Description
		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(s)	The user(s) or group(s) assigned to the trust store.
	Approver(s)	Browse to specify the user(s) or groups(s) that can approve workflows assigned to this trust store.
Certificate Trust Bundles	Certificate Trust Bundles	Specify the Trust Bundles associated with this trust store. To learn more about Trust Bundles, see "Managing certificate bundle objects" on page 341.
Provisioning Interval	Disable Scheduled Provisioning	Select Yes or No to disable provisioning for this trust store.
	Provision Every	If you selected Yes above, specify how often provisioning should occur.
Application Information	Application Credential	Browse for the credential object that you want to use to authenticate with the application
	Connection Method	Click SSH.
	Port	Specify the associated port number for the Connection Method.

Settings		Description
Trust Store Settings		
PKCS#12	Trust Store Path	Specify the path to the file that is being Provisioned.
	Trust Store Credential	A password is required in order to add or remove certificates from the keystore. In the Credential Selector list, choose the appropriate stored credential.

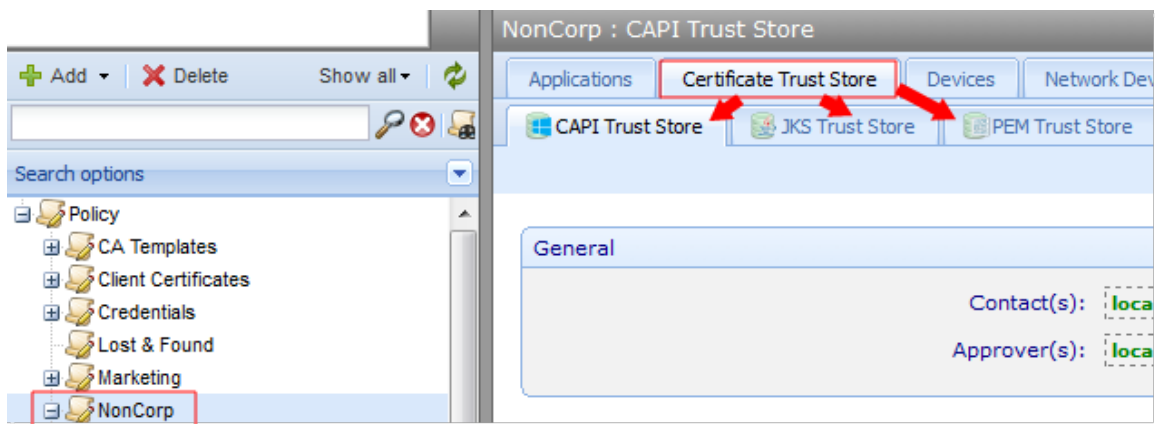
- When you're finished, click **Save**.

Adding a trust bundle to a trust store

You can bundle certificates together and whitelist or blacklist them, and then add the bundle to a trust store. For more details, see ["Creating and managing trust stores"](#) on page 348.

Add a trust bundle to a trust store on a policy

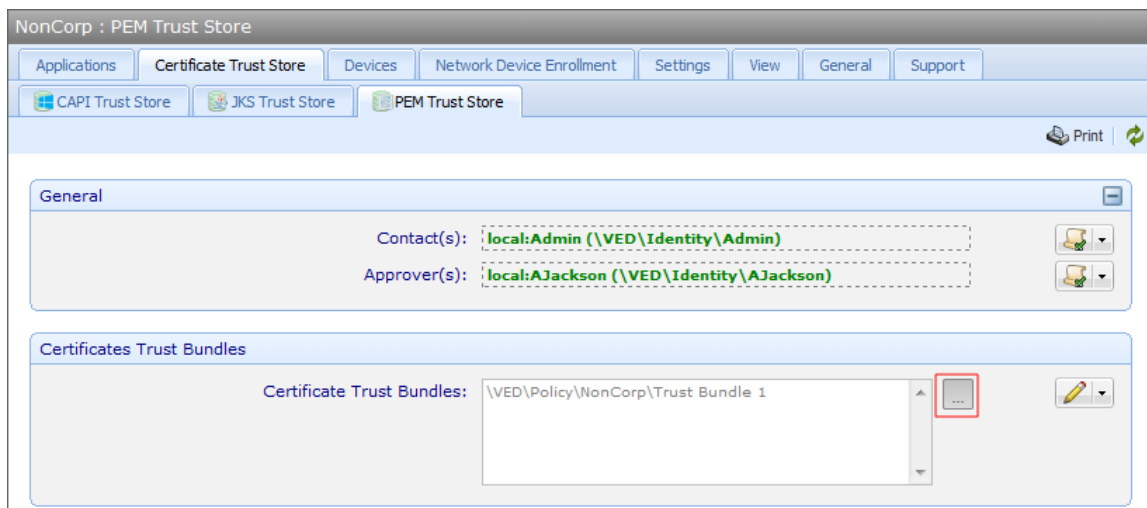
- Click the policy you want then click the **Certificate Trust Store** tab. The types of Trust Stores that are available are displayed in the next row of tabs.



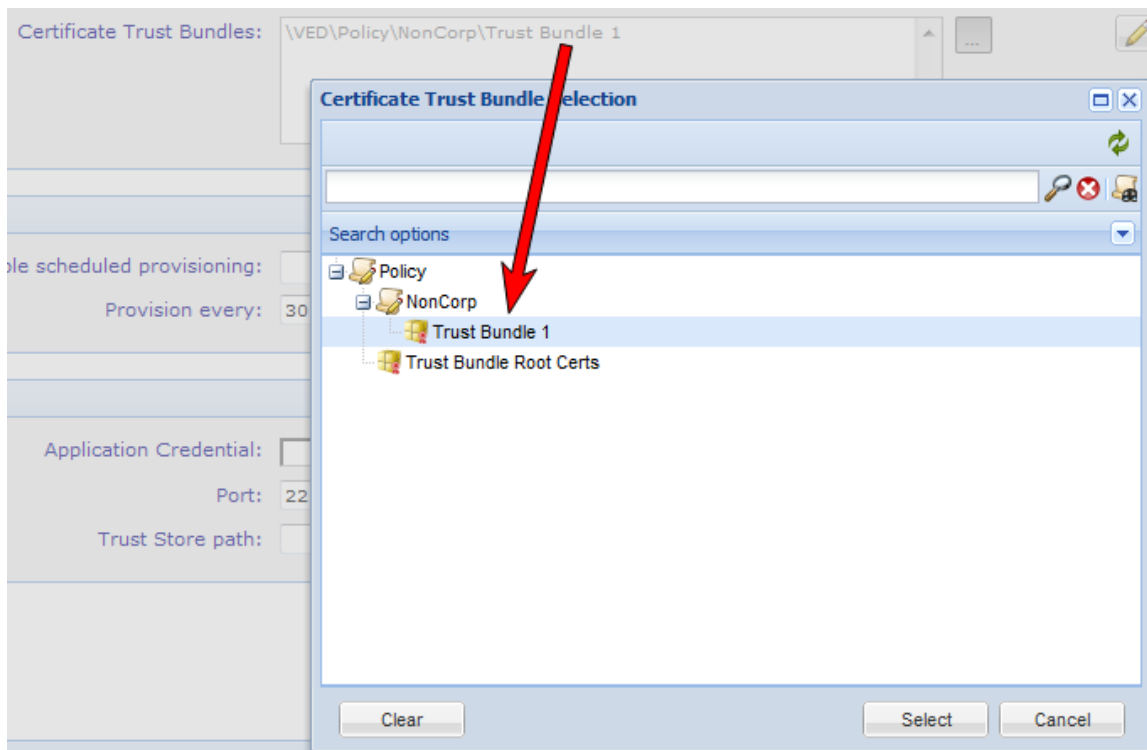
- Click the type of Trust Store to which you want to add the bundle.

Adding a trust bundle to a trust store

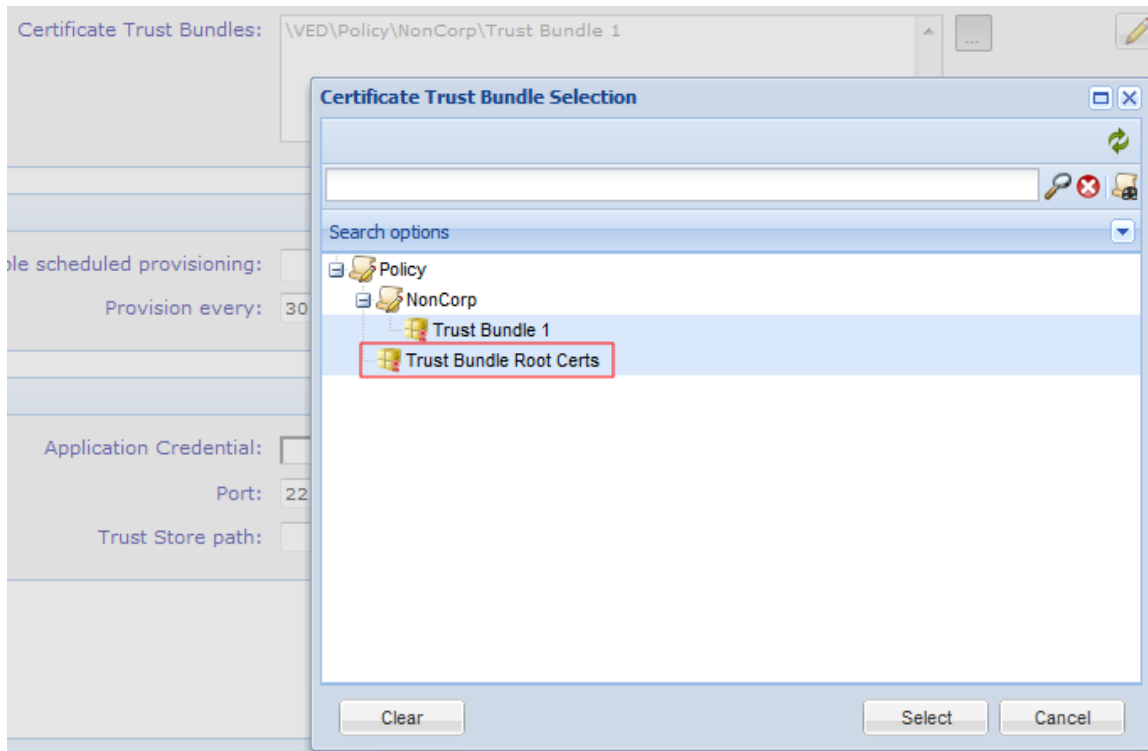
3. Click Browse  in the Certificate Trust Bundle group box.



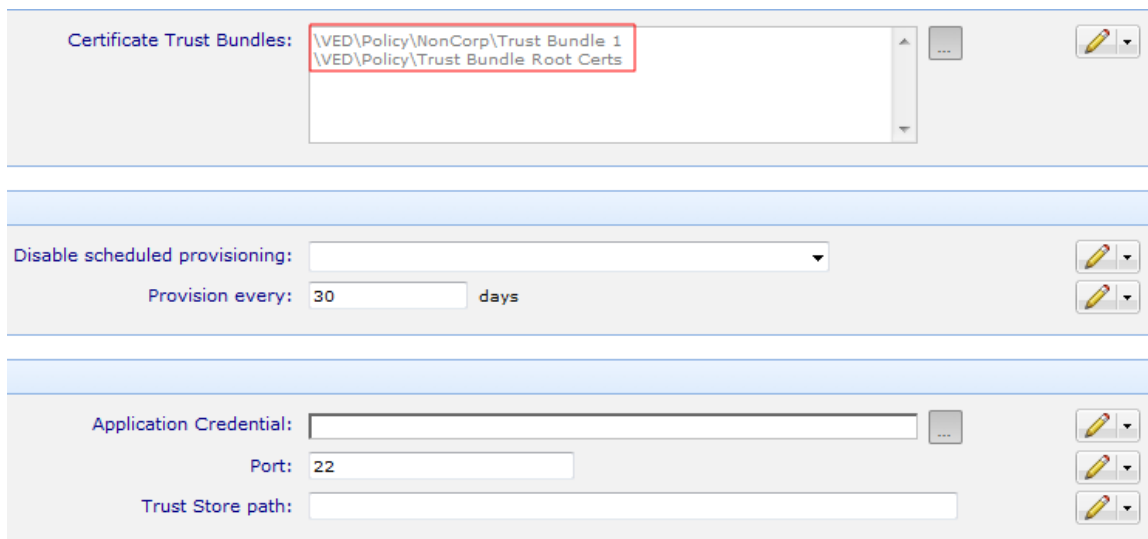
4. In the **Selection** window, bundles that are already in the trust store will be highlighted when the window is opened.



5. Press Shift + CTRL to highlight other trust bundles you want to add.

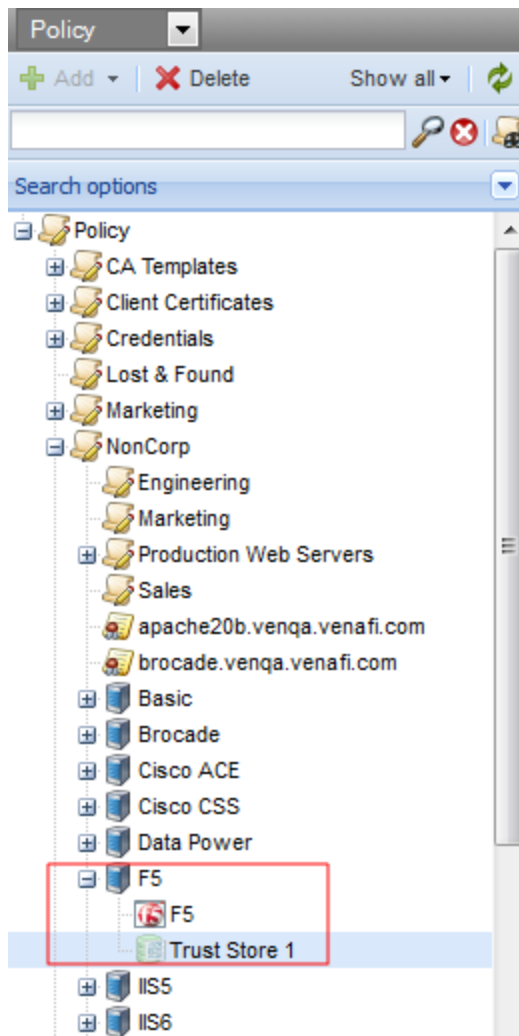


6. When all trust bundles are added, click **Select**.
7. The list of all trust bundles in the Trust Store is displayed.

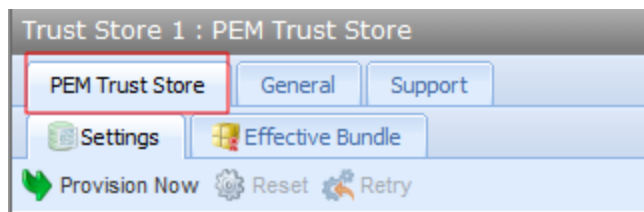


Add a trust bundle to a trust store already on a device

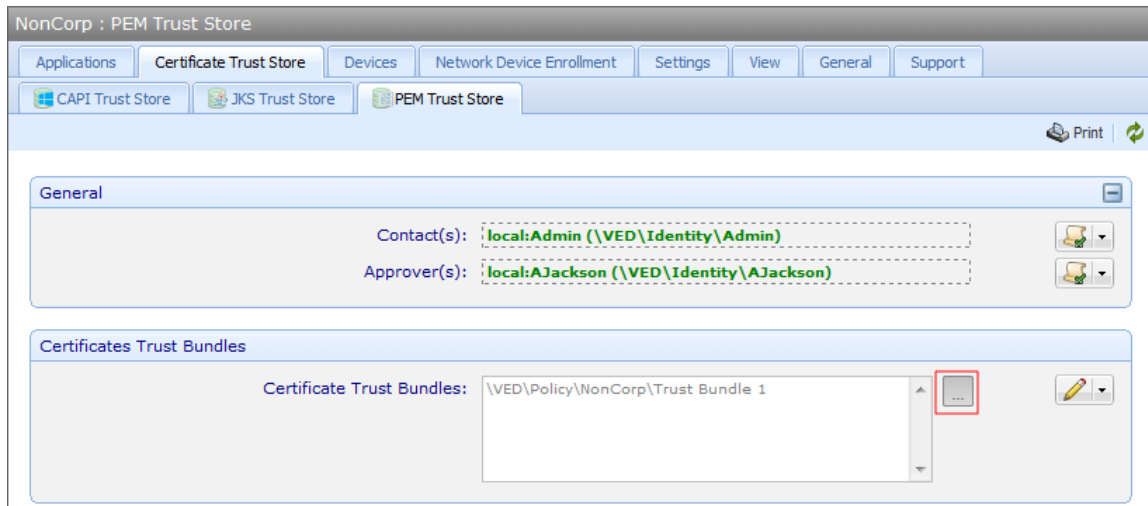
1. Click the device, and then click **Trust Store**.



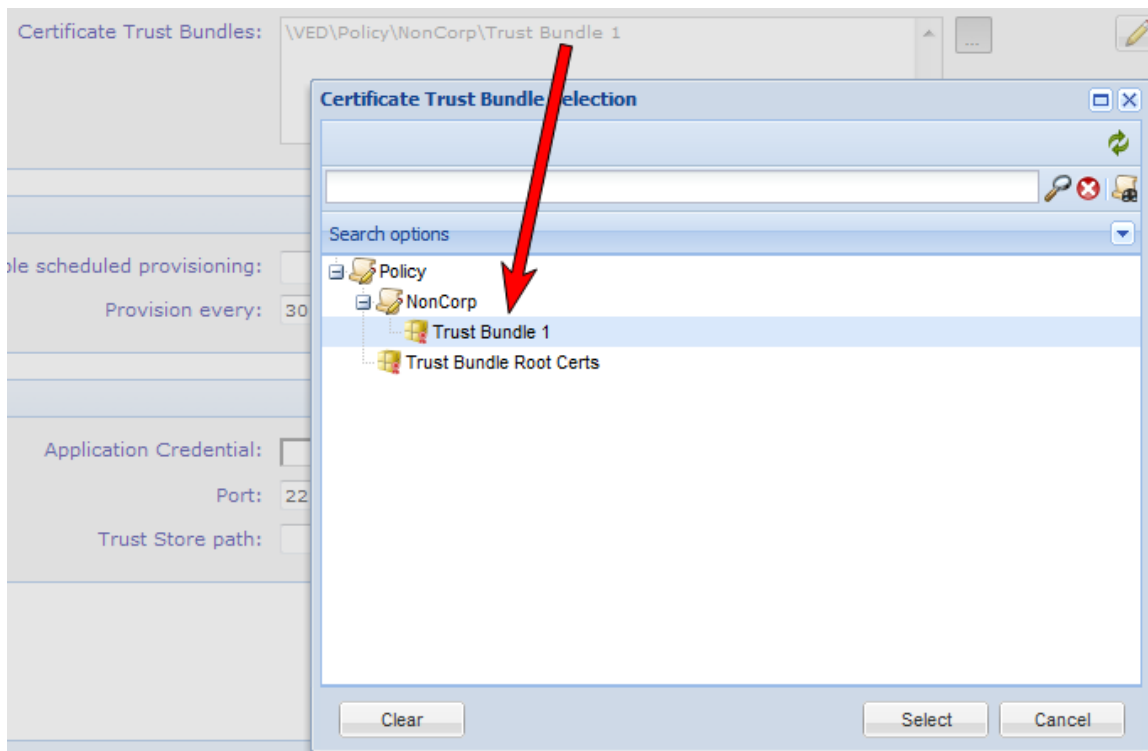
2. Click the Trust Store tab.



3. Click Browse  in the Certificate Trust Bundle group box.

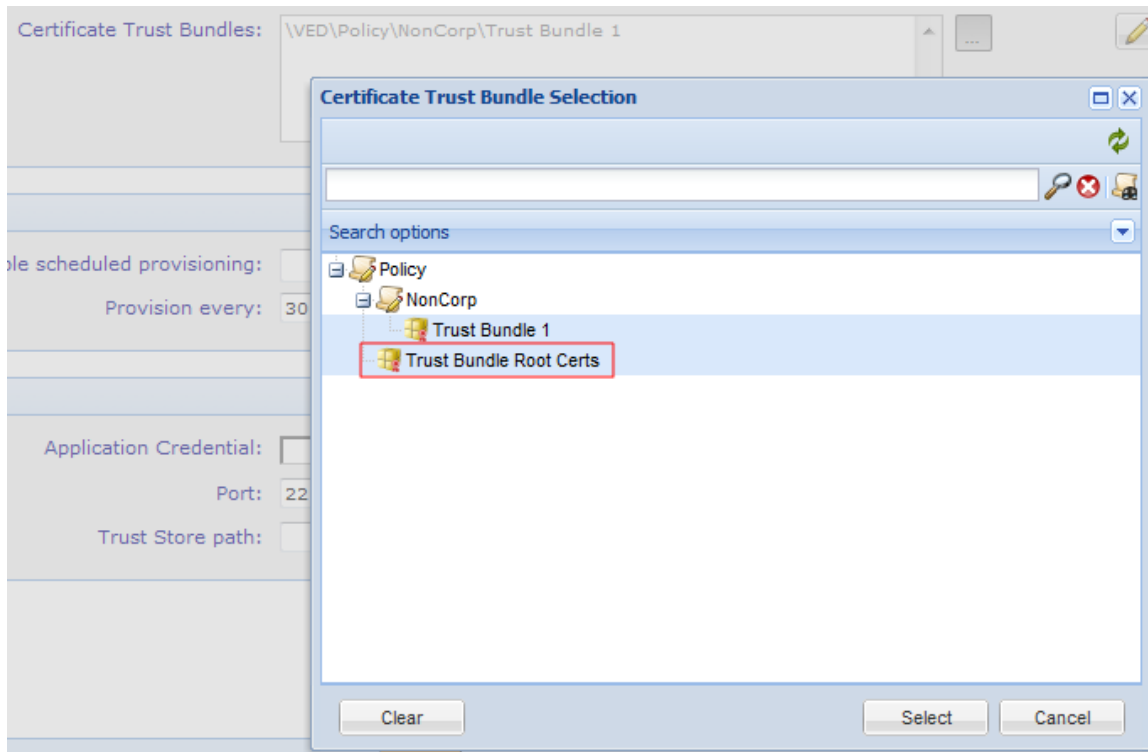


4. In the **Selection** window, bundles that are already in the trust store will be highlighted when the window is opened.



5. Press Shift + CTRL to highlight other trust bundles you want to add.

Adding a trust bundle to a trust store



6. When all trust bundles are added, click **Select**.
7. The list of all trust bundles in the trust store is displayed.

Trust Store 1 : Settings

PEM Trust Store General Support

Settings Effective Bundle

Provision Now Reset Retry Print

Status

Status: **Ok**

Processing Stage: **none**

Last Provisioned: **never**

Processing Disabled: ☐

General

Description:

Contact(s): local:Admin (\VED\Identity\Admin)

Approver(s): local:AJackson (\VED\Identity\AJackson)

Certificates Trust Bundles

Certificate Trust Bundles: VED\Policy\NonCorp\Trust Bundle 1
VED\Policy\Trust Bundle Root Certs

Provisioning Interval

Disable scheduled provisioning:

Provision every: 30 days

Application Information

Save

Provisioning bundles to trust stores

You can provision trust bundles that are installed on Trust Stores. Provisioning helps you secure and protect your trust assets because certificates are automatically monitored, renewed, and installed.

See "Certificate installation" on page 493 in the *Trust Protection Platform Certificate Management Guide*.

Creating a certificate workflow

Workflow objects define the parameters required to implement a workflow approval or inject a local command at a specific stage of the certificate lifecycle.

You must have the *Create* permission to the policy where you want to create the workflow.

To create a Workflow object

1. From the **Platform** menu bar, click Policy Tree.
2. Select the policy for which you want to create the workflow.
3. Click **Add > Workflow**.

The Detail View displays the Workflow's associated settings.

Add New : Workflow

Print

General

* Name:

Conditions

* If Stage is:

If Application or Trust Store is:

Actions

Inject Commands: ☐

Commands:

Commands will be evaluated for macros. If the command includes a single "\$", and is not intended to be used as a macro, then "\$" should be replaced with "\$\$."

Request Approval: ☐

Request Approval From: ☒ Approver assigned to object
☐ Specified approver
☐ Specify approver via macro

Specified Approver(s):

Approver Macro:

Approval Reason Code:

Save

4. In the **Name** field, enter a friendly name.
5. In the **Conditions** box, enter the qualifying conditions.

Setting	Description
If Stage Is	Enter the condition stage when the workflow event should be triggered. Stages are listed below.
If Application or Trust Store is	Will only trigger the approval if the certificate is installed on the Application or Trust Store selected from the list. If selected, this condition is in addition to the Stage Code. (That is to say there is an implied AND operation between the conditions.)

Certificate workflow Stage Codes

Certificate Stage Codes

Stage Code	Friendly Name	Description
0	StartProcessing	Prepares the certificate for lifecycle processing.
100	CheckStore	Applies only to remote generations. If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.
200	CreateConfigureStore	Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object.
300	CreateKey	Creates the private key. DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400.

Stage Code	Friendly Name	Description
400	CreateCSR	Creates the Certificate Signing Request (CSR). If Service Generated CSR is enabled and the certificate is associated with multiple applications, the CSR will be centrally generated so Trust Protection Platform can push the private key to multiple applications.
500	PostCSR	Submits the CSR to the Certificate Authority (CA). If you post a manual CSR, this is the first stage of the certificate lifecycle.
600	ApproveRequest	Approves the certificate renewal at the CA.
700	RetrieveCertificate	Retrieves the certificate from the CA.
800	InstallCertificate	Installs the certificate on the target application. This provisioning happens in several stages, such as 801, 802, etc. All stages between 800-899 are provisioning stages.
900	CheckConfiguration	Reserved for future use. You cannot apply this stage to a workflow.
1000	ConfigureApplication	Reserved for future use. You cannot apply a stage to this workflow.
1100	RestartApplication	Used for command injection workflow that must be executed after a certificate has been successfully provisioned.
1200	EndProcessing	Completes the certificate processing and, if configured, runs a Validation check on the certificate and application.

Stage Code	Friendly Name	Description
1400	Revocation	Submits a revocation request to the CA. Certificate revocation is a certificate operation; it does not involve the application driver.
1500	UpdateTrustStore	Updates the Trust Store at the host to comply with the effective bundle. To learn more, see "Viewing the Effective Bundle" on page 346.
1600	EndTrustStoreProcessing	Completes the processing of the Trust Store.

NOTE If there are multiple approvals set at the same stage, all approvals will trigger at the same time, and all approvals must be resolved before the workflow can continue. In Aperture, if a user is an approver for multiple workflow tickets at the same stage, approving or rejecting any of the workflow tickets will have the same effect on all workflow tickets assigned to the same object and stage.

6. In the **Actions** box, enter the appropriate actions.

Setting	Description
Inject Commands	Under the designated conditions, Trust Protection Platform executes the defined commands on the certificate's consumer application. Trust Protection Platform is able to run local SSH commands against the following applications: ◦ A10 AX Traffic Manager ◦ Apache ◦ F5 LTM Advanced ◦ IBM GSK ◦ Imperva MX ◦ JKS ◦ Layer 7 SSG ◦ Oracle iPlanet ◦ PEM ◦ PKCS#12 ◦ Tealeaf PCA Trust Protection Platform is able to run PowerShell commands over WinRM for the CAPI application. After Trust Protection Platform executes the command, the application driver logs an Inject Command Success or Inject Command Failure event so you can determine if the command successfully executed on the target application. The Inject Command Success event returns a value of zero (0) in the event's Value2 field. An Inject Command Failure event returns a non-zero numeric value in the Value2 field. To provide automatic notification for Inject Command Failure events, you can create a Notification Rule that triggers on a value greater than zero in the event's Value2 field. For more information, see "Creating notification rules" on page 432 in the <i>Venafi Trust Protection Platform Administration Guide</i>.
Request Approval	Check the box to request approval when this workflow condition is triggered.
Request Approval From	Select the source of the approver. ◦ Approver assigned to the object. For certificates, this is defined by the certificate settings in the Policy Tree.

Setting	Description
	◦ Specified approver. Hard-code the approvers to be used. Activates the Specified Approver(s) field where you must enter the identities used for the approval. If multiple approvers are added, all listed approvers must approve the workflow item before it will be approved. If any of the approvers rejects the workflow, the item will be rejected. ◦ Specify approver via macro. Allows you to enter a macro to dynamically select the workflow approver when the workflow is triggered. For more information on the Trust Protection Platform macro language, see the <i>Venafi Trust Protection Platform Macro Guide</i>. Activates the Approver Macro field where you must enter the macro command.
Approval Reason Code	Enter the Reason Code you want to include with the notification that is sent to the workflow approver. The maximum Approval Reason Code value is 999. IMPORTANT This option is required if you select Request Approval From. Approval Reason Codes also accompany customized explanations or instructions for workflow approvers. The drop-down list displays the Reason Codes defined in the Workflow tree. For more information, see "Defining reason codes for certificate approvals" on page 573.

7. Click **Save**.

IMPORTANT When you define a Workflow object that requires approval, you must also select an Approval Reason Code to provide explanations or instructions for the workflow approvers. To learn more, see ["Defining reason codes for certificate approvals" on page 573](#).

For a detailed description of the object settings, see ["Workflow object settings" on page 565](#).

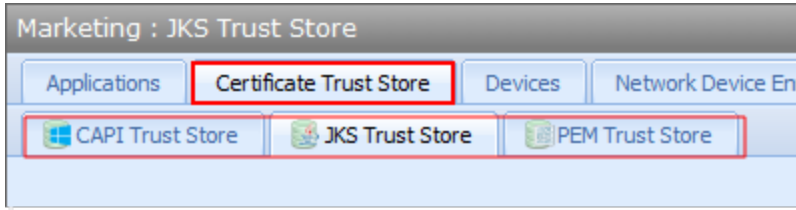
Enabling regular updates for compliance

You can set Trust Protection Platform to automatically update a Trust Store by scheduling regular updates or provisioning. Scheduling provisioning helps ensure compliance with corporate folders.

To learn more, see ["Certificate Installation \(Provisioning\) – Trust Force™" on page 26](#).

To schedule provisioning for a trust store

1. From the **Policy** tree, click the policy, and then click **Certificate Trust Store**.
2. Click the Trust Store you want to provision.



3. In the **Provisioning Interval** group box:
4. **Disable Scheduled Provisioning:** Select **No** to enable provisioning or **Yes** to disable provisioning for the Trust Store.
5. **Provision Every:** If **No** was selected, enter the number of days between provisioning events.

6. When you're done, click **Save**.

About Domain Whitelisting

Domain whitelisting offers powerful security enhancements you set at the policy level.

- Control over which domain suffixes can be used in new certificate requests
- Prevents non-compliant certificates from being issued by internal certificate authorities (CAs)
- Prevents wildcard certificates from being used (or limits who is authorized to have wildcard certificates), and
- Prevents potential man-in-the-middle attacks and other nefarious activity by ensuring that new certificate requests don't contain duplicate certificate names

NOTE If the domain name does not match any of the Allowed Domains as defined in the Domain Whitelist at the time of attempted enrollment, adjusting the domains requested for the certificate and attempting enrollment again will clear the risk.

To learn more about configuring domain whitelisting using Policy Tree, see ["About certificate object settings"](#) on page 146.

To learn more about domain whitelisting, see ["Setting policy on a folder"](#) on page 177.

9

Managing certificate notifications

In addition to cataloging and monitoring your organization's certificates, Venafi Trust Protection Platform™ can notify key contacts or other individuals prior to the expiration date of the certificate. If a certificate is not renewed in a timely manner—15 days prior to expiration, for instance—escalation notifications can be sent to other individuals to ensure the certificate is renewed before it expires.

Notification messages can be relayed to key custodians using SMTP or SNMP traps and, for audit purposes, they can be logged to an MS SQL database as well as an individual log file. Implementing Trust Protection Platform notifications as part of your certificate management strategy facilitates effective certificate management and provides an audit trail for the implementation of corporate security folders.

This chapter contains the following topics:

About certificate notification and logging	394
Notification and logging overview	394
Setting up notifications and logging	395
Notification object settings	396

About certificate notification and logging

Venafi Trust Protection Platform™ provides real-time monitoring and notification so you can assess and act on events as they occur. Trust Protection Platform collects event data from encryption assets distributed across multiple systems and platforms so you can review and evaluate your encryption system activity. Flexible notification and escalation functionality sends dynamically-generated messages to object contacts, approvers, or other relevant stake holders.

Notification and logging overview

The recipients and delivery method for certificate expiration notifications are defined in Notification and Channel objects. You must configure the Channel and Notification objects to send notifications for certificate expiration events.

Event logging and notifications are managed using Notification and Channel objects. Based on criteria you define in the Notification object, Trust Protection Platform selects specific types of events and sends those events to one or more designated channels.

Channel objects define the event output target. For example, the SMTP channel provides the information Trust Protection Platform needs to output an event to an email message; the SNMP channel defines the parameters required to output an event as an SNMP trap; and the File and MS SQL channels provide the information required to write events to a log store.

In addition to the Notification and Channel objects, you must configure your Venafi Log server and Log Store (Default SQL Channel object) to enable certificate expiration notifications and logging.

The Venafi Log server manages the flow of information to the Default SQL Channel object, interprets Notification Rules, and uses Channels to deliver events based on those rules. It receives incoming events, then logs all events to the Default SQL Channel to ensure there is a complete audit trail of all system operations and events. Once an event is logged to the Default SQL Channel, the Log server determines if the event matches the criteria of any notification rule. If there is a match, the Log server forwards the event to the appropriate channels.

The Default SQL Channel object is the central repository where the Venafi Log server writes all logging events. The Default SQL Channel is created during installation as a table in the Trust Protection Platform database; however, if you choose, you can use a database other than the Trust Protection Platform database as the Default SQL Channel.

The Venafi Log server, Notification and Channel objects, including the Default SQL Channel, are created and managed in the Logging tree. 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.

Setting up notifications and logging

The following high-level procedure outlines the configuration requirements for enabling logging and notification for certificate management and SSH workflows.

To set up notifications and logging

1. Configure the Venafi Log server.

For further information on the Log server configuration, see [Managing the Log server](#) in the *Venafi Trust Protection Platform Administration Guide*.

2. Configure the Default SQL Channel object.

The Default SQL Channel is created during installation as a table in the Trust Protection Platform database. If you choose to use a database other than the Trust Protection Platform database as the Default SQL Channel, you must configure the associated database and table structure. You must also provide the new database connection settings in the Default SQL Channel object and reconfigure the Default Channel definition in the Log Server object. For more information on these configurations, see [Managing the Default SQL Channel object](#) in the *Venafi Trust Protection Platform Administration Guide*.

3. Configure the default SMTP options in the root Channel object in the Logging tree.

For information on these settings, see [Setting up notification channels](#) in the *Venafi Trust Protection Platform Administration Guide*.

4. Configure the target Channel objects to which you want to forward your notification events.

You can define your own Channel objects or use the default Channel objects provided in the Channels folder. The following table provides a description of just a few of the default Channel objects that are relevant to expiration notifications:

Default Channel Object	Description
Email to Consumer (SMTP)	Emails a notification message to the contacts assigned to the applications that consume the target certificate. This channel is used to provide notification for certificate expiration events.
Email to Owner (SMTP)	Emails a notification message to the certificate contacts. This channel is used provide notification for certificate expiration events.
Email to Parent (SMTP)	Emails a notification message to the contacts assigned to the target certificate's parent object. This channel is used to provide notification for certificate expiration and Discovery survey events.
Email to Ticket Approver (SMTP)	Emails an approval request to a workflow ticket approver. This channel provides workflow approval request notifications.

For information on Channel object configuration, see [Setting up notification channels](#) in the *Venafi Trust Protection Platform Administration Guide*.

5. Configure notification rules to provide notifications for certificate and SSH events.

For steps on managing notification rules, see [Managing notification rules](#)

For an explanation of the notification rule object settings, see ["Notification object settings"](#) on page 430.

Notification object settings

The following table outlines the settings for Notification Rule objects.

Field	Description
Settings	
Disabled	Disables the current Notification Rule object. If the Notification object is disabled, the Log server ignore the rule and no notifications are sent.
Rule	
Event Field	Defines the Notification Rule criteria. The event field that contains the data you want to use to select events.

Field	Description
	For more information about the event fields, see Managing event structure and log schema in the <i>Venafi Trust Protection Platform Administration Guide</i> .
Condition	Condition under which the Log server applies the value to the event field. Depending on the event field, you can select one of the following conditions from the drop-down list box: ▪ Matches: Event field matches the designated value. ▪ Is less: Event field is less than the designated value. ▪ Is more: Event field is more than the designated value. ▪ Is between: Event field is between the two designated values. ▪ Contains: Event field contains the designated value. ▪ Has RegEx Match: Data in the event field matches the pattern in the designated regular expression query. For more information on regular expressions, see Using regular expressions in a notification rule in the <i>Venafi Trust Protection Platform Administration Guide</i>.
Value	Value for the designated event field. The Venafi Log server applies the value to the designated event field under the defined conditions. If an event matches the criteria, it is sent to the designated notification channel.
Operators	To narrow the selection results, you can define values for multiple event fields. Using standard AND, NOT, and OR operators. The conditions are cumulative; that is, the Log server applies the first condition, then the second, then the third, etc., to progressively narrow the results.
Target Channels	Channel objects the Venafi Log server uses to provide event responses or log the events. You can select multiple notification channels for any given Notification Rule object.

Field	Description
Add	Adds new Channel objects for event notification.
Remove	Removes selected Channel objects from the notification rule.
permissions	On the object permissions tab, you select the users or groups you want to have 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 Notification Rules folder. If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

10

Working with lost certificates

Venafi Trust Protection Platform helps you and your certificate managers find and claim lost certificates. After lost certificates are brought under management, they're easy to monitor, enroll, and provision.

This chapter contains the following topics:

Finding assets using filters on the Certificate Inventory list.....	400
Check for Lost Certificates.....	417
About Identities and Permissions.....	420
About Notifications.....	428
Account settings for expiring certificates.....	437

Finding assets using filters on the Certificate Inventory list

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.

On the Certificate Inventory, you must click the **Apply Filters** button at the top of the filter sidebar to see changes applied. This helps you by allowing you to specify multiple filter criteria before applying the filter and running the filter query, saving you time when working with certificates.

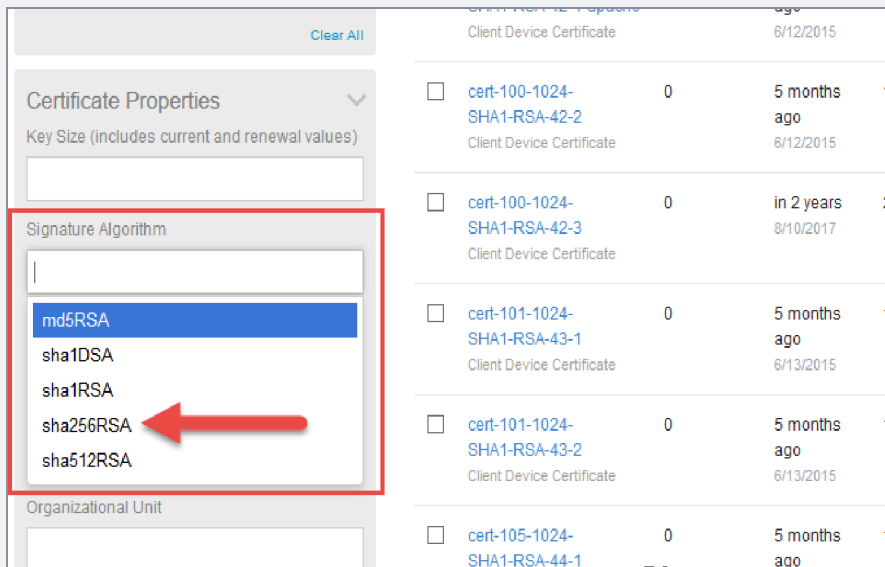
Filter Panel Groups and Filter Types

The filter panel contains the following filter groups:

- **Quick Filters.** These are built-in filters provided by the system that help you identify common issues with your keys and certificates.
- **Common Filters.** These are filter fields that you will commonly use to find a specific item.
- **Certificate Properties.** This is a detailed list of all certificate properties, allowing you to filter on any property on the certificate. You can learn more about certificate properties in ["About certificate object settings" on page 146](#).
- **Validation.** This is a list of validation properties, allowing you to filter the certificates based on their validation results.
- **Discovery.** This is a list of filters that allow you to find certificates based on discovery information.

EXAMPLE Show all certificates with a specific signature algorithm.

Suppose you need to filter the **Inventory > Certificates** list in TLS Protect to show only user certificates with a signature algorithm of sha256RSA. Click Certificate Properties and then select **sha256RSA** from the **Signature Algorithm** drop-down list, then click **Apply Filters**.



The screenshot shows the 'Certificate Properties' dialog box in the TLS Protect interface. The 'Signature Algorithm' dropdown menu is open, displaying a list of algorithms: md5RSA, sha1DSA, sha1RSA, sha256RSA, and sha512RSA. A red arrow points to 'sha256RSA', which is the selected option. The background shows a table of certificates with columns for 'Certificate', 'Expiration', 'Days to Expiration', and 'Days to Renewal'. The table lists several certificates, including 'cert-100-1024-SHA1-RSA-42-2', 'cert-100-1024-SHA1-RSA-42-3', 'cert-101-1024-SHA1-RSA-43-1', 'cert-101-1024-SHA1-RSA-43-2', and 'cert-105-1024-SHA1-RSA-44-1'.

Certificate	Expiration	Days to Expiration	Days to Renewal
cert-100-1024-SHA1-RSA-42-2	6/12/2015	5 months ago	10
cert-100-1024-SHA1-RSA-42-3	8/10/2017	in 2 years	20
cert-101-1024-SHA1-RSA-43-1	6/13/2015	5 months ago	10
cert-101-1024-SHA1-RSA-43-2	6/13/2015	5 months ago	10
cert-105-1024-SHA1-RSA-44-1	-	5 months ago	10

EXAMPLE Show which agents have not checked in for awhile.

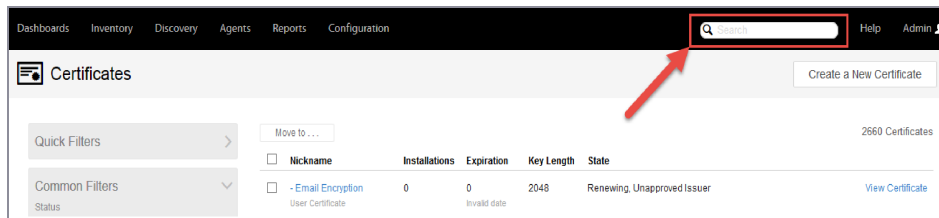
Suppose you need to know which Server Agents have not checked in to Trust Protection Platform for the past 30 days. In TLS Protect, click **Clients > Registered Clients** on the menu bar to open the Registered Clients list view. All registered clients (which you must have permissions to view) appear in the list according to the default search criteria. To find the items that meet your unique criteria, apply the Not Seen In filter by setting it to 30 days. The list would then instantly update to display only those registered clients that have not checked in within the past 30 days.

To search for Objects using quick search

NOTE Quick Search does not allow you to search for agents.

1. In the **Search** box on the menu bar, type all or part of the name of the object you are looking for, and then press the Enter key.

Finding assets using filters on the Certificate Inventory list



2. In the search results, click the name of an object to view its details.

To refine a list of discovered objects Using Filters

1. From the menu, open any of the inventory list views.

For example, click **Inventory > Certificates**, or click **Clients > Registered Clients**.

2. Using Filters, select and apply one or more filters to narrow the list of discovered items.

DID YOU KNOW? On the Certificate Inventory, you can add multiple filter criteria without refreshing the list. When your filter criteria are correct, click **Apply Filters** (at the top of the filter sidebar). This feature saves time when working with large certificate inventories.

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 (with the exception of Status [found only on the Certificates inventory page], which is an **AND** field).

The screenshot shows a filter interface with three sections:

- Policy Tree Location:** Contains two selected filters: "Policy \ EMEA" and "Policy \ EMEA \ Mktg". A "Clear" link is visible.
- Certificate Type:** Contains two selected filters: "Server Certificate" and "Client Device Certificate". A "+" icon and a "Clear" link are visible.
- Certificate Properties:** Contains two selected filters: "Disabled" and "Expired - Long Term". A "Clear All" link is visible.

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 Quick Filters for Certificates

The following Quick Filters are available on the Certificate Inventory page.

Quick Filter	Description
Lost & Found	Loads certificates with the <i>Lost</i> risk.
Pending My Approval	Loads certificates with the <i>Pending My Approval</i> status. For these certificates, you are listed as the approver, and they are waiting for your approval.
In Error	Loads certificates with the <i>In Error</i> status. Click the information icon to see details about each certificate's error. Alternatively, you can use the Edit Columns link to add the <i>Error Details</i> column to always display the error information.

Quick Filter	Description
Expiring Soon	Loads certificates with the <i>Expiring Soon</i> status.
Distrusted Entrust	Loads certificates that are distrusted by some web browsers because they are issued by one of the following CAs: ▪ Entrust ▪ AffirmTrust

List of Common Filters for Certificates

The following Common Filters are available on the Certificate Inventory page.

Common Filter	Description	Multi-value Support	Type
Status	Filters the certificate list to show only certificates that match a given status. For more information on certificate status see " Certificate status and risks explained " on page 37.	Yes / AND	Select from list
Risks	Filters the certificate list to show only certificates that match a given risk. The risk you filter on may apply to a certificate, but may not be displayed in the Risks column, due to the display priority of the risk condition .	Yes / AND	Select from list
Certificate Name	Searches the object name, the common name of the current certificate, and the common name renewal value.	No	Partial match search (starts with)

Common Filter	Description	Multi-value Support	Type
Certificate Authority Template	Filters the certificate list based on the most recent CA template used on the certificate. This will show all certificates currently linked to that CA template. This filter is based on renewal settings for certificates that have been renewed.	Yes / OR	Select from list
Serial Number	Filters based on the certificate's serial number.	Yes / OR	Partial match search (contains)
Contacts	Filters based on the certificate's contact name or group. You can select multiple contacts, if needed.	Yes / OR	Search from list
Approvers	Filters based on the approver name or group.	Yes / OR	Search from list
Installation Type	Filters based on the installation type assigned to a certificate. In addition, you can also filter on certificates that have at least one installation of any type by selecting the "Any" option from the list. You can also filter on certificates with zero installations by selecting "None" from the list.	Yes / OR	Select from list
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	Search from list
Last Renewed By	Filters based on the user who was the last one to renew the certificate.	Yes / OR	Search from list

List of Certificate Properties

The following are a list of certificate properties filters available in the Certificate Inventory.

Certificate Property	Description	Multi-value Support	Type
Key Size	The size of the key represents the relative strength of the key, with larger numbers representing more secure keys.	Yes / OR	Select from list
Signature Algorithm	The key algorithm associated with the certificate	Yes / OR	Select from list
Validity Period	Duration of validity for the certificate, allowing you to, for example, quickly see certificates with long validity periods, which represent higher risk than certificates with a shorter validity period.	Yes / OR	Select from list
Organization	Name of the organization listed on the certificate.	Yes / OR	Select from list
Organizational Unit	Name of the organizational unit listed on the certificate.	Yes / OR	Select from list
City/Locality	City listed on the certificate.	Yes / OR	Select from list
State/Province	State listed on the certificate.	Yes / OR	Select from list
Country	Country listed on the certificate.	Yes / OR	Select from list
Domain Component	If enabled by policy, and if used by the certificate, the domain components allowed by the certificate.	Yes / OR	Select from list
Issuer	Name of CA, organization, or device that issued the certificate. Allows "Self-signed" to show all self-signed certificates	Yes / OR	Select from list
SANs - DNS	The fully qualified domain name or common name associated with the certificate. Filter results will be displayed for search term found anywhere in the name (i.e. starts with, ends with, or contains).	Yes / OR	Search from list

Certificate Property	Description	Multi-value Support	Type
Validation Result	Status of the most recent validation attempt for the certificate installation.	Yes / OR	Select from list
Management Type	The level of certificate management in Trust Protection Platform: unassigned, monitoring, enrollment, or provisioning.	Yes / OR	Select from list
Certificate Type	The type of certificate; for example, server certificate, user certificate, or client device certificate.	Yes / OR	Select from list
Key Algorithm	RSA Algorithm used by the key tied to the certificate.	Yes / OR	Select from list
Elliptic Curve	Which elliptic curve is used for the certificate.	Yes / OR	Select from list
Valid From	First date that the certificate was valid. Can specify a specific date range, or a dynamic date range (next 60 days)	Date Range	Explicit or dynamic range
Valid To	Last date that the certificate is valid. Can specify a specific date range, or a dynamic date range (next 60 days)	Date Range	Explicit or dynamic range

List of Validation Filters

The following are a list of Validation filters available on the Certificate Inventory

Validation Filter	Description	Multi-value support	Type
Overall Result	Filter certificates based on whether validation for the certificate's endpoints either succeeded or failed.	Yes / OR	Select from list
Enabled Protocols	Filter certificates based on the protocols enabled for a certificate's endpoints. (For example, TLS 1.2 or TLS 1.3)	Yes / OR	Select from list
SSL/TLS Chain Result	Filter certificates based on the chain validation result for a certificate's endpoints. Possible chain results include: CA certificate omitted, chain not valid, expiring CA in chain, etc.	Yes / OR	Search from list
SSL/TLS End Entity Result	Filter certificates based on the End Entity validation result. Possible end entity results include: Connection failure, Hostname not resolvable, network validation not supported, no certificate match, no local certificate, etc.	Yes / OR	Select from list

List of Discovery Filters

The following are a list of Discovery filters available on the Certificate Inventory. Use the Discovery filters to locate objects added by a network discovery job specified in the filter.

You need Read/View permission to select objects in the filter. You must set these permissions on \\VED\Discovery or on the job object.

Discovery Filter	Description	Multi-value support	Type
CA Trust Monitor	Whether the CA trusts or distrusts the certificate.	Yes / OR	Select from list
ACME Public Key Fingerprint	The public key fingerprint (for ACME certificates).	Yes / OR	Select from list
Added to Inventory by	The method that was used to add the certificate to the inventory. (E.g. Agent Discovery, Aperture, Network Discovery, WebSDK).	Yes / OR	Select from list
Certificate Origin	The originator of the certificate. This filter is available only if Client Protect has been licensed.	Yes / OR	Select from list
Network Discovery Job	The network discovery job Note: When you select Last Scan Certificates Only , the filter will display only those objects that were modified by the last discover scan.	Yes / OR	Select from list
Created On	Date the certificate was created. Can specify a specific date range, or a dynamic date range (next 60 days)	Date Range	Explicit or dynamic range

Find certificates assigned to a specific user

You can find certificates that are assigned to specific users by using either Quick Search or Filters.

Using quick search

1. From Trust Protection Platform's menu bar, click the **magnifying glass**.
2. Enter the user's first name, last name, username, or email address in the **Search** field, and then press Enter.

You'll see a list of users whose names match your search criteria along with their associated certificates.

3. Click the certificate name to see details about the certificate..

Finding assets using filters on the Certificate Inventory list

Steady			10 Certificates
Nickname	Expiration	State	
A Shore in Common Name User Certificate	In 12 Months 10/7/2014		Download ▾
AShore - No SAN Client Device Certificate	In 11 Months 9/11/2014	Validation Disabled	Download ▾
AShore UPN User Certificate	In 11 Months 9/11/2014		Download ▾
AShore UPN-Email User Certificate	In 11 Months 9/11/2014		Download ▾
AShore-Client Client Device Certificate	In 11 Months 10/5/2014	Validation Disabled	Download ▾

- Click the certificate's name to view its details.

[Certificates](#) / [A Shore in Common Name](#)

A Shore in Common Name

User Certificate

Download

Issuer	Common Name	Organization	Organizational Unit	Locality	State / Province	Key Size
Self Signed	ashore	Venafi Inc.	Development	Salt Lake City	Utah	1024

Key Usage: Enhanced Key Usage
Digital Signature, Key Encipherment (a0) Smart Card Logon (1.3.6.1.4.1.311.20.2.2), Client Auth...

EXPIRATION

350 Days Left 10/7/2014

✗ Renewal Disabled

[Schedule Renewal](#)
[Renew Now](#)
[Retire](#)
[Revoke](#)

Show All Properties

Using Filters

NOTE As your filter selection changes, your search results change with it.

- From the TLS Protect menu bar, click **Inventory > Certificates**.
- In the **User Name** field, type one of the following:

- a. First name
- b. Last name
- c. User name
- d. Email address

You'll see a list containing certificates for that user. You can take action on a certificate directly from this screen. Use the drop-down arrow to see more actions.

3. Click the certificate name to see details about it.

Expired Long Term
Download

AShore - UPN - 1day Download

User Certificate | Template: Cert Based Auth - Upn - 1day

Issuer	Common Name	Organization	Organizational Unit	Locality	State / Province	Key Size
VenQA Class G CA	AShore	Venafi, Inc	Venafi	Salt Lake City		2048

Key Usage Digital Signature, Non-Repudiation, Key Encipherment (e0)	Enhanced Key Usage Client Authentication (1.3.6.1.5.5.7.3.2)

EXPIRATION

40 Days Ago
9/12/2013

✖
Renewal Disabled

[Schedule Renewal](#)
[Renew Now](#)
[Retire](#)
[Revoke](#)

SUBJECT ALTERNATIVE NAMES

Other

- Principal Name : AShore@venqa.venafi.com

Show All Properties

Editing columns in the Certificate Inventory list

When you're viewing the certificate inventory list, you can add, delete, and reorder the columns. You can refine the information that's displayed so that you can see just the certificates you're interested in. You can also edit columns when you create a Custom Report. To learn how, see [Creating a new custom report](#).

To edit columns in the Certificate Inventory list

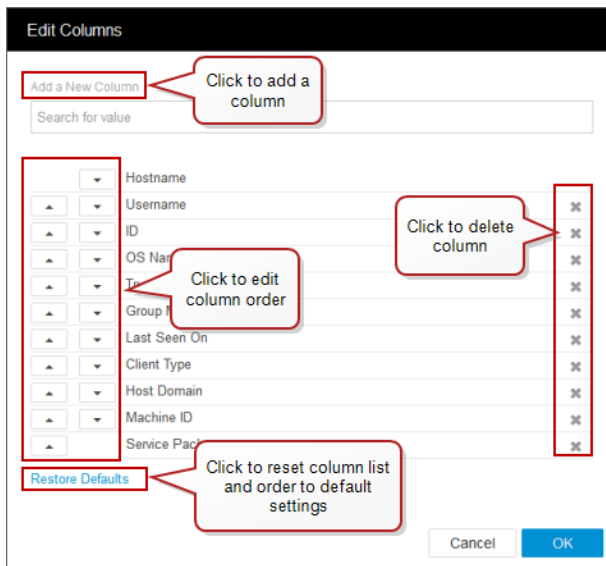
1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. Click **Edit Columns**.



3. In the **Edit Columns** window, make the desired changes.

You can add, remove, or reorder columns.

The column order will be stored in your user profile, so when you refresh or revisit the page, your preferred columns will be displayed. At any point, if you want to reset the column list and order to the default settings, click the **Restore Defaults** link.



TIP You can also reorder columns using drag and drop.

4. When you're done, click **OK**.

About the arrows in column headers

☐ Nickname ▾ Installations Expiration ▾ Key Length ▲ Status City ▾ State/Province ▾

Arrow	What it means
Grey arrow	Sortable, but not sorted
Black arrow	Sorted
Arrow pointing up	Sorted A-Z
Arrow pointing down	Sorted Z-A

All Columns that can be added

Column Name	Sortable?
Approvers	No
Certificate Type	Yes
City	Yes
Common Name	Yes
Contacts	No
Country	Yes
Custom Fields - Date/Time	No
Custom Fields - Identity	No
Custom Fields - List Multi	No
Custom Fields - List Single	Yes
Custom Fields - String	Yes

Column Name	Sortable?
Days to Expiration	Yes
Description	Yes
DN	Yes
Domain	Yes
Elliptic Curve	Yes
Error Details	No
Folder	Yes
In error	Yes
Installations	No
Issuer	No
Key Algorithm	Yes
Key Size	Yes
Last Renewed By	No
Management Type	No
Manual CSR Required	Yes
Nickname	Yes
Organization	Yes
Organizational Unit	No
Renewal Date	No

Column Name	Sortable?
Reputation Score	Yes
Retired	Yes
Revocation Status	No
Risk	No
Sans (DNS)	No
Sans (Email)	No
Sans (IP)	No
Sans (UPN)	No
Sans (URI)	No
Serial Number	Yes
Signature Algorithm	Yes
State/Province	Yes
Status	No
TLS Endpoints	No
Valid From	Yes
Valid To	Yes
Validation Enabled	No
Validation Result	No
Validity Period	No

Columns that contain nested data

The **Installations** column and the **TLS Endpoints** column can display nested data. Click the down arrow to see the related data displayed in a table. If you click another column's nested data button, that data will replace the nested data shown. Only one nested data table can be displayed at a time.

Installations nested data

When you add the **Installations** column to your inventory list, you see the number of installations associated with the certificate. Click the down arrow to view installations for an individual certificate. Once the nested table is displayed, click the X to collapse the data.

Available columns for the **Installations** sub table are:

- Installation Type
- Device
- Contacts
- Installation Status
- SSL/TLS Validation Port

TLS Endpoints nested data

When you add the **TLS Endpoints** column to your inventory list, you see the number of TLS endpoints associated with the certificate. Click the down arrow to view the devices connected to the certificate. Once the nested table is displayed, click the X to collapse the data.

Available columns for the **TLS Endpoints** sub table are:

- IP Address
- Port
- Protocols
- SSL/TLS Validation
- Chain Validation

NOTE The TLS Endpoints column is available to be included in Custom Reports.

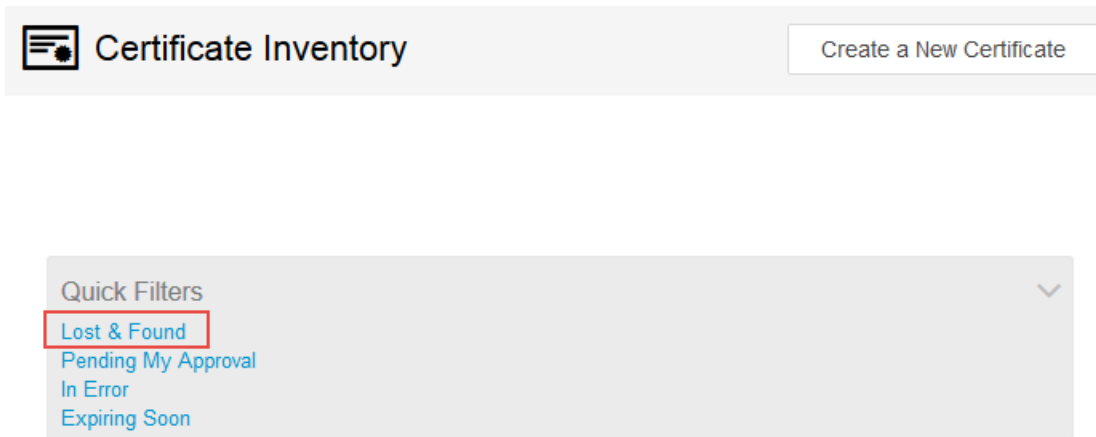
Check for Lost Certificates

If you're logging in to TLS Protect for the first time, you should check the Lost & Found for certificates that may require immediate attention.

Certificates whose owner the Trust Protection Platform Administrator couldn't identify were placed here.

To check for lost certificates

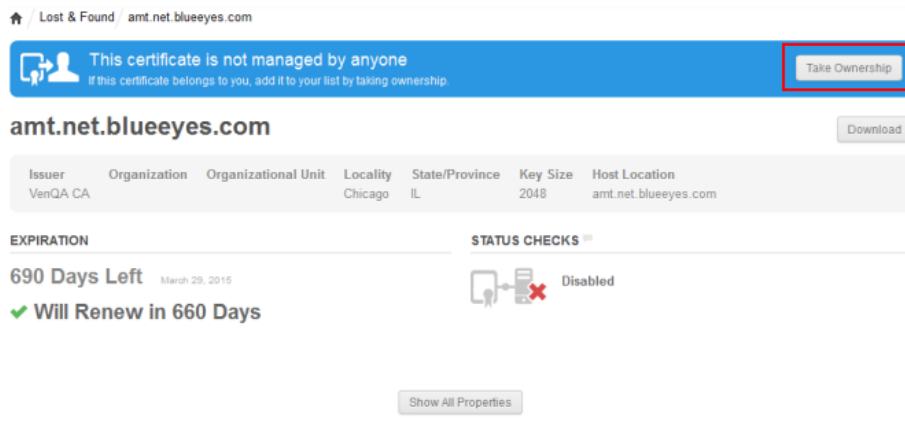
1. Log in to TLS Protect.
2. On the menu bar, click **Inventory > Certificates**.
3. Under Quick Filters, click **Lost & Found**



4. From the list of Lost certificates, you can **Take Ownership**.

To take ownership from the certificate details page

1. Click the certificate's name to see its details.
2. On the details page, click **Take Ownership**.

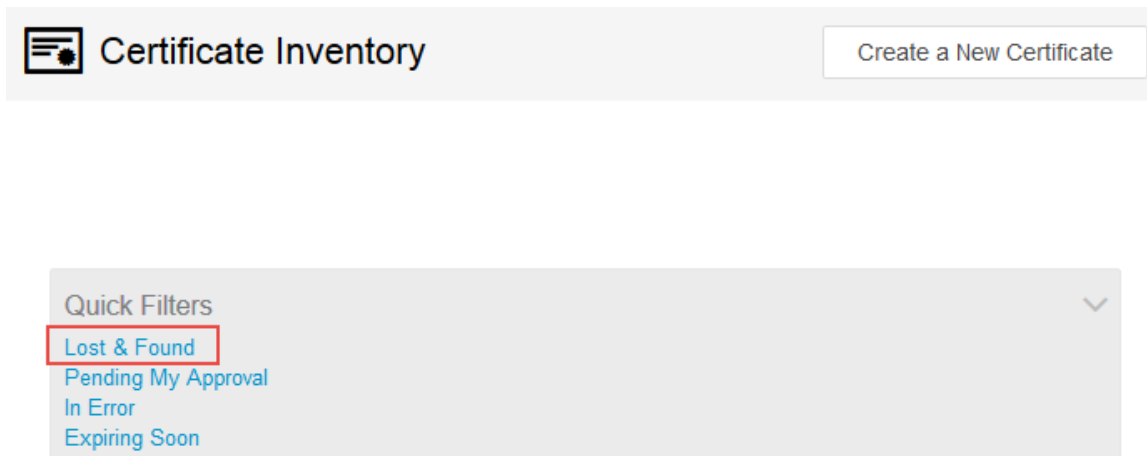


Taking ownership of a lost certificate

Trust Protection Platform identifies certificates that have no owner. From the list, you can take ownership of a lost certificate.

To take ownership of a lost certificate

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. To see Lost certificates, in **Quick Filters**, select **Lost & Found**.



3. From the list of Lost certificates, click **Take Ownership**.

Certificate Inventory Create a New Certificate

38 of 38 Certificates

Certificate Names

Enter a common name

Clear

Expires Between

Clear

Custom Field

Select field name

Clear

Policy Tree Location

Select a location

Clear

Certificate Type

Clear

Certificate Properties Clear All

Status

Lost x

Clear

Key Size

Move To...

☐	Nickname	Expiration	Key Length	State	
☐		in 2 months 5/20/2015	2048	Lost, Validation Disabled	Take Ownership
☐		6 months ago 8/30/2014	2048	Lost, Expired - Long Term, Failed Validation, Revoked	Take Ownership
☐		in 3 years 6/13/2018	2048	Lost, Unsafe Validity Period, Validation Disabled	Take Ownership
☐		9 months ago 6/11/2014	2048	Lost, Expired - Long Term, Failed Validation, Validation Disabled	Take Ownership
☐		in 2 months 5/13/2015	2048	Lost	Take Ownership
☐		tomorrow 3/7/2015	2048	Lost, Awaiting CSR, In Error, Renewing, Expiring Soon	Take Ownership
☐		tomorrow 3/7/2015	2048	Lost, Awaiting CSR, In Error, Renewing, Expiring Soon	Take Ownership
☐		in 12 months 3/5/2016	2048	Lost, Failed Validation, Validation Disabled	Take Ownership

- Use the drop-down arrow to choose a policy to move the certificate to.
- Click **OK**.

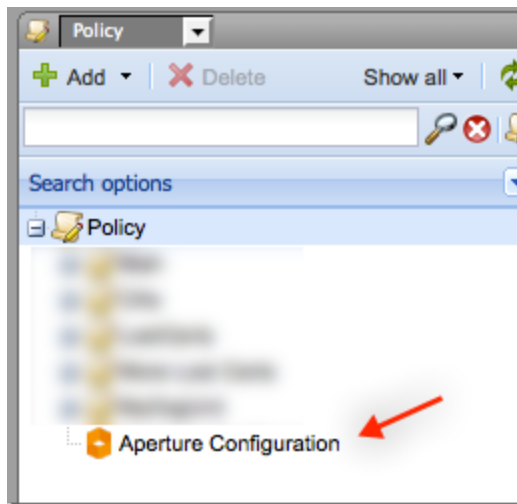
You'll see a confirmation that the certificate has been moved to the designated policy.

NOTE Depending on how ownership is defined by your company, an owner can be anyone who is a Contact or has *Read* and *Write* permissions for the new policy. In this case, taking ownership means moving the certificate from a central **Lost** policy to an existing policy.

About the Aperture configuration object

When you installed Aperture, the Aperture Configuration object was automatically created. There can be only one Aperture Configuration object but you can move it around in the Policy tree.

In Policy Tree, you can specify general settings for this object. For more information, see [Set up the configuration object in the Trust Protection Platform](#).



About Identities and Permissions

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.

You must explicitly grant permissions to users before they can manage objects.

"Setting up Identities" below

"Assign Permissions to Identities (users and groups)" on page 422

Setting up Identities

The first thing to do is set up an Identity so that you can assign permissions and allow access to appropriate folders. You can also add a group as an Identity.

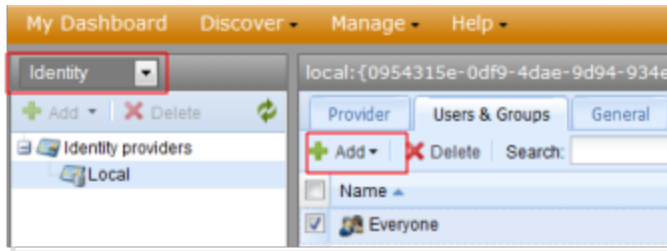
Remember, Trust Protection Platform can link to your existing Active Directory (AD) to help you set up users and groups.

Why is this important?

Think about who your certificate managers are and which folders and certificates they manage. First, you want to make sure that each certificate manager or group has an Identity because you'll soon be assigning permissions to enable them to see certain certificates and folders. Then, you may want to organize users and groups in a way that makes it easy to see their access level at a glance. For details about how to use Identities in Trust Protection Platform, see [Working with identities, permissions, and teams](#) in the *Venafi Trust Protection Platform Administration Guide*.

Set up an Identity

1. From the TLS Protect menu bar, click Policy Tree.
2. Open the **Identity** tree.



3. Define the user's information (first name, last name, email address, and the like).

The screenshot shows the 'Users & Groups' management interface. At the top, there are tabs for 'Provider', 'Users & Groups', and 'General'. Below these are controls for adding, deleting, and searching users, along with a record limit and export options. A table lists several users: Petejo, Sally, Spencer (selected), Support, and Western region. Below the table, the 'Details' section for the selected user 'Spencer' is shown. It includes fields for 'Full Name', 'First Name', 'Last Name', 'Email', 'Password', and 'Confirm Password'. The 'WebSDK Access' checkbox is checked and highlighted with a red box. A 'Save' button is located at the bottom of the form.

4. Click **Save**.
5. Repeat this process for other users and groups, as needed.
6. Now, set up the Lost & Found folders in Trust Protection Platform. Doing this allows a user to access the Lost & Found folders and CA objects that he or she needs to work with.

Assign Permissions to Identities (users and groups)

Now that you've set up your Lost & Found folders, it's time to assign Identity permissions, based on role, to enable access to those folders. You can also assign permissions to access individual certificates.

In our example, Spencer will need permissions to the Lost & Found folders you just set up. He'll also need permissions to the folders that he'll move his certificates to when he takes ownership of them.

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 <i>Read</i> permissions to the certificate can see only the associated applications to which they have <i>View</i> or higher permissions to the Application object. In Application objects, users with <i>Read</i> permissions to the application can see only the associated certificate if they have <i>View</i> or higher permissions to the Certificate object. For SSH keysets, users with <i>Read</i> 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 <i>Read</i> 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 <i>Write</i> permissions to the objects and <i>Create</i> permissions to the target folder. <i>Read</i> permissions are inferred. Rename is selected by default but can be deselected. In Certificate and Application objects, the user also has access to the following options in the designated pages:		
	<table> <tr> <td>Certificate Summary Page</td><td>Users with <i>Write</i> permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.</td></tr> </table>	Certificate Summary Page	Users with <i>Write</i> permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.
Certificate Summary Page	Users with <i>Write</i> permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.		

Permission	Allows the user to...
Certificate Settings Page	Users with <i>Write</i> permissions to the Certificate object have access to the Renew Now option.
Certificate Associations Page	Users with <i>Write</i> permissions to the Certificate object can see all associated applications, regardless of their permissions to the individual applications. Users with <i>Write</i> permissions to the Certificate object can add associations only to those applications to which they have either <i>Write</i>, or both <i>Associate</i> and <i>View</i> permissions. Users with <i>Write</i> permissions to the Certificate object have access to the Retry Installation option only for those applications to which they have either <i>Write</i> or both <i>Associate</i> and <i>View</i> permissions. Users with <i>Write</i> permissions to the Certificate object can push the certificate and private key only to those applications to which they have either <i>Write</i> or both <i>Associate</i> and <i>View</i> permissions. Users with <i>Write</i> permissions to the Certificate object can enable or disable the certificate only on those applications to which they have either <i>Write</i> or both <i>Associate</i> and <i>View</i> permissions.
Application Settings Page	Users with <i>Write</i> permissions to the Application object can add associations only if no certificate is currently associated with the Application object or if they have either <i>Write</i> or both <i>Associate</i> and <i>View</i> permissions to the associated Certificate object.

Permission	Allows the user to...
	Users with <i>Write</i> permissions to the Application object have access to the Retry Installation option only if they have either <i>Write</i> or <i>Associate</i> and <i>View</i> permissions to the associated Certificate object. Users with <i>Write</i> permissions to the Application object can push the certificate and private key to the application only if they have either <i>Write</i> or <i>Associate</i> and <i>View</i> permissions to the associated Certificate object. For SSH keys, users with <i>Write</i> 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 <i>Write</i> 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. <i>View</i> is inferred. For SSH keys, you must have the <i>Create</i> permission in the target folder to move a keyset into that folder.
Manage Policy	Lets users modify policy values on folders. <i>Read</i> and <i>Write</i> permissions are implied; the <i>View</i> permission is not. In order for the Manage Policy permission to be useful, users should be granted the <i>View</i> 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.

Permission	Allows the user to...
	For SSH keys, you need to have the <i>Delete</i> permission to remove keysets from all folders (returning the keyset to device-level permissions). For SSH keys, you need the <i>Delete</i> 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 <i>Create</i> permission in the target location. When an object is moved, locked policy attributes are recalculated.
Associate	If you have <i>Write</i> permissions to a Certificate object and both <i>Associate</i> and <i>View</i> 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, renew, process, or validate certificates for the current application. If you have <i>Write</i> permissions to an Application object and <i>Associate</i> and <i>View</i> 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.

Permission	Allows the user to...
	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 <i>Write</i> 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.
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 <i>Manage Permissions</i> .
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 <i>Admin</i> .

Give users permissions to Lost & Found folders

TIP Before you start, it's a good idea to map out user and group permissions to ensure there aren't any collisions or gaps.

1. Go to the **Policy** tree, and click a policy that you specified as Lost & Found.
2. Click **General** and then click **Permissions**. Grant a minimum of **View**, **Read**, and **Rename** permissions to your Lost & Found folders.
3. Give other users additional permissions as needed. Refer to the **Rename** permission in the table above.

Give users permissions to folders to which they will move certificates

When users "take ownership" of a lost certificate, they will be asked to which policy the certificate should be moved. They may also want to give the certificate a new name.

1. Give users **View**, **Read**, **Write**, and **Create** permissions to the folders to which the certificates will be moved.

When you grant a user the **Create** permission to a policy, it gives the user the ability to create a certificate under that policy.

2. Repeat until you have given Aperture users their appropriate permissions.
3. When you're done, click **Save**.

EXAMPLE Let's say you want Spencer to be able to see certificates in a Lost & Found policy then be able to move them to Policy 1 or Policy 2. Give Spencer *View*, *Read* and *Rename* permissions to the Lost & Found policy then give him *View*, *Read*, *Rename* and *Create* permissions to both Policy 1 and Policy 2.

You're almost done! The last step is to specify the folders and certificates to be managed by Aperture. You can do this manually or allow Trust Protection Platform to automatically configure the setting when a lost certificate is claimed or a new certificate is created.

Next step: See [Specify folders and certificates to be managed by Aperture](#) in the *Trust Protection Platform Certificate Management Guide* .

About Notifications

Using Trust Protection Platform's notification system, TLS Protect can notify key contacts or other individuals about key actions that need to be taken. Notification emails can be sent to certificate managers via SMTP or SNMP and, for audit purposes, can be logged to an MS SQL database as well as an individual log file. Using notifications keeps your certificate managers informed and provides an audit trail for corporate security folders.

"Setting up notifications and logging" below

"Notification object settings" on the next page

"Customizing email notifications" on page 432

Setting up notifications and logging

The following high-level procedure outlines the configuration requirements for enabling logging and notification for certificate management and SSH workflows.

To set up notifications and logging

1. Configure the Venafi Log server.

For further information on the Log server configuration, see [Managing the Log server](#) in the *Venafi Trust Protection Platform Administration Guide*.

2. Configure the Default SQL Channel object.

The Default SQL Channel is created during installation as a table in the Trust Protection Platform database. If you choose to use a database other than the Trust Protection Platform database as the Default SQL Channel, you must configure the associated database and table structure. You must also provide the new database connection settings in the Default SQL Channel object and reconfigure the Default Channel definition in the Log Server object. For more information on these configurations, see [Managing the Default SQL Channel object](#) in the *Venafi Trust Protection Platform Administration Guide*.

3. Configure the default SMTP options in the root Channel object in the Logging tree.

For information on these settings, see [Setting up notification channels](#) in the *Venafi Trust Protection Platform Administration Guide*.

4. Configure the target Channel objects to which you want to forward your notification events.

You can define your own Channel objects or use the default Channel objects provided in the Channels folder. The following table provides a description of just a few of the default Channel objects that are relevant to expiration notifications:

Default Channel Object	Description
Email to Consumer (SMTP)	Emails a notification message to the contacts assigned to the applications that consume the target certificate. This channel is used to provide notification for certificate expiration events.
Email to Owner (SMTP)	Emails a notification message to the certificate contacts. This channel is used provide notification for certificate expiration events.
Email to Parent (SMTP)	Emails a notification message to the contacts assigned to the target certificate's parent object. This channel is used to provide notification for certificate expiration and Discovery survey events.
Email to Ticket Approver (SMTP)	Emails an approval request to a workflow ticket approver. This channel provides workflow approval request notifications.

For information on Channel object configuration, see [Setting up notification channels](#) in the *Venafi Trust Protection Platform Administration Guide*.

5. Configure notification rules to provide notifications for certificate and SSH events.

For steps on managing notification rules, see [Managing notification rules](#)

For an explanation of the notification rule object settings, see "Notification object settings" below.

Notification object settings

The following table outlines the settings for Notification Rule objects.

Field	Description
Settings	
Disabled	Disables the current Notification Rule object. If the Notification object is disabled, the Log server ignore the rule and no notifications are sent.
Rule	
Event Field	The event field that contains the data you want to use to select events.

Field	Description
	For more information about the event fields, see Managing event structure and log schema in the <i>Venafi Trust Protection Platform Administration Guide</i> .
Condition	Condition under which the Log server applies the value to the event field. Depending on the event field, you can select one of the following conditions from the drop-down list box: ▪ Matches: Event field matches the designated value. ▪ Is less: Event field is less than the designated value. ▪ Is more: Event field is more than the designated value. ▪ Is between: Event field is between the two designated values. ▪ Contains: Event field contains the designated value. ▪ Has RegEx Match: Data in the event field matches the pattern in the designated regular expression query. For more information on regular expressions, see Using regular expressions in a notification rule in the <i>Venafi Trust Protection Platform Administration Guide</i>.
Value	Value for the designated event field. The Venafi Log server applies the value to the designated event field under the defined conditions. If an event matches the criteria, it is sent to the designated notification channel.
Operators	To narrow the selection results, you can define values for multiple event fields. Using standard AND, NOT, and OR operators. The conditions are cumulative; that is, the Log server applies the first condition, then the second, then the third, etc., to progressively narrow the results.
Target Channels	Channel objects the Venafi Log server uses to provide event responses or log the events. You can select multiple notification channels for any given Notification Rule object.

Field	Description
Add	Adds new Channel objects for event notification.
Remove	Removes selected Channel objects from the notification rule.
permissions	On the object permissions tab, you select the users or groups you want to have 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 Notification Rules folder. If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Customizing email notifications

You can customize the email notifications that are sent to individuals in your company. You can even change the look, feel, and branding of your email notifications.

Email notifications are managed through the SMTP channels in Venafi Configuration Console (VCC).

The actual messages that are delivered are a combination of e-mail templates, SMTP channel settings, and notification rules. When an event fires, if there is a matching notification rule, then the SMTP channel connected to that notification rule is triggered. The SMTP channel is linked to an email template, which contains the images and style settings used to send the message.

The specifics of how this process works is outlined in [SMTP channel](#). Here are some specific topics to get you started.

- [Email templates](#)
- [Managing logos and images used in email templates](#)
- [About SMTP templates for email notifications](#)
- [Editing SMTP message templates](#)

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.

Field	Description
	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)	<code>a == b</code>	Compares if <code>a</code> is equal to value <code>b</code> . Returns <code>true</code> if they are equal, otherwise returns <code>false</code> .
!= (Not Equals)	<code>a != b</code>	Compares if <code>a</code> is not equal to value <code>b</code> . Returns <code>true</code> if they are not equal, otherwise returns <code>false</code> .
IN	<code>a in [0010, 0020, 0030]</code>	Checks if value <code>a</code> is present in the specified <code>[group]</code> . Returns <code>true</code> if it is, otherwise returns <code>false</code> . The group is a comma separated list inside square brackets.
IS	<code>a IS EMPTY</code>	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	<code>MATCHES "\\\\VED\\\\Policy\\\\.*"</code>	Argument is a regular expression and variable must have a match to be TRUE.

¹String arguments should be entered with quotation marks.

²Regular expressions are only supported using the `MATCHES` operator, and use .NET regular expression syntax. See [Using regular expressions in a notification rule](#).

Operator	Syntax ¹	Description
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.

Variable	Example	Rules						
		==	!=	<	<=	>	>=	
Component	\VED\Policy\Abc	✓				✓	✓	✓
Data ²	Some Text					✓	✓	✓
EventID	0x001f0003	✓		✓				
Grouping	154	✓		✓				✓

¹String arguments should be entered with quotation marks.

²Data is assumed to be encoded UTF-8 text and converted to UTF-8 before operators are applied.

Variable	Example	Rules					
		==	!=	<	<=	>	>=
Severity	Info	✓		✓			✓
SourceIP ¹	192.168.3.4/24	✓				✓	✓
Text1	Some Text	✓				✓	✓
Text2	Other text	✓				✓	✓
Value1	123	✓		✓			✓
Value2	456	✓		✓			✓

Account settings for expiring certificates

You can easily configure how expired or expiring items should be handled.

To configure account settings

1. Click your user name.
2. Click **Account Settings**.
3. Enter the desired number of days, and then click **Save**.

Account Settings

Available Settings

Mark items that have been expired for more than days as Expired - Long Term

Mark items that are expiring in less than days as Expiring Soon

Cancel

Save

¹SourceIP supports both IPv4 and IPv6 addresses and CIDR notation.

11

Working with certificates

Venafi Trust Protection Platform helps you and your certificate managers with tasks that keep your certificates current and valid. This section helps you with common certificate-related tasks.

This chapter contains the following topics:

Creating a new certificate	440
Taking action on a certificate	447
Working with certificate installations	475
Running validation scans	486
How certificate renewal works	489
Sorting certificates in the Policy Tree Certificates grid	490
About Domain Components	491

Creating a new certificate

Creating a new certificate is not difficult, but it's a good idea to review the [certificate object settings](#) to familiarize yourself with information you'll need to provide when you create the certificate request.

IMPORTANT You must have the *View*, *Read*, *Write*, and *Create* permissions in order to complete this task.

To create a new certificate

1. In the TLS Protect menu bar, click **Inventory > Certificates**.
2. Click **Create a New Certificate**.
3. In **Create a New Certificate**, enter information into each of the tabs, as described below.

Folder Tab

- a. Select the location where you want to store the certificate in the **Certificate Folder**, then click **Submit**.

- b. Enter the **Nickname**, which must be unique in the given folder.

This usually matches the certificate's Common Name.

Object names may not contain the backslash \ or less-than sign < characters. Object names (including their path ancestors in the policy tree) must be fewer than 255 total characters.

- c. (Optional) Enter a **Description** for the certificate you are creating.
- d. Select the **Management Type**.

NOTE Depending on what you select on this field, options on the following screens will be slightly different.

- e. Fill out other fields, including any custom fields, as needed, then click **Next**.

Certificate Signing Request tab

- a. Select the **Hash Algorithm**.
- b. Choose the **CSR Generation** method.

If you chose **Enrollment** on the previous screen:

- i. If you are generating your own CSR:
 - i. Paste the CSR into the **Enter CSR** field.
 - ii. If there are any policy issues with the SAN types, you will need to either resolve them by creating a new CSR with SAN types that match the policy, or move the certificate to another folder which allows the SAN types specified in the CSR.
 - iii. If there are any policy issues with domain components, you will need to either resolve them by creating a new CSR with domain components that match the policy (or, if the policy doesn't allow domain components, create a CSR without domain components), or move the certificate to another folder whose domain components policy match the ones specified in the CSR.

Click **Next**. Skip to the next tab's instructions in the next section.

- ii. If you are having Trust Protection Platform generate the CSR:
 - i. Enter a **Common Name** and then fill out the organization and location fields.
 - ii. If allowed by policy, specify the domain component(s) that apply to this certificate.

If this setting is not allowed by policy, this field will be hidden. For more information on domain components, see ["About Domain Components"](#) on page 491.
 - iii. Choose a **Key Algorithm** and **Key Size**.

To see a comparison chart, see ["About RSA and elliptic curve cryptography \(ECC\) key algorithms"](#) on page 446.

For help selecting an algorithm, see ["Choosing a key algorithm based on the certificate authority \(CA\)"](#) on page 443.
 - iv. Click **Next**.

If you chose **Provisioning** on the previous screen:

- i. Choose your **Key and CSR Generation Options**.

The recommended option will be selected. For more information about remote versus central key generation, see [Supported methods of key generation](#) in the Administration Guide.

- ii. Enter a **Common Name** and then fill out the organization and location fields.

- iii. If allowed by policy, specify the domain component(s) that apply to this certificate.

If this setting is not allowed by policy, this field will be hidden. For more information on domain components, see ["About Domain Components"](#) on page 491.

- iv. Choose a **Key Algorithm**, and if necessary, an **Elliptic Curve**.

To see a comparison chart, see ["About RSA and elliptic curve cryptography \(ECC\) key algorithms"](#) on page 446.

For help selecting an algorithm, see ["Choosing a key algorithm based on the certificate authority \(CA\)"](#) on the facing page.

- v. Click **Next**.

Additional Information tab

- a. Enter the Subject Alternative Names (SANs).

The SAN types available will depend on the policy settings that are applied to the folder you selected for this certificate. If permitted by policy, you can enter SANS information for the following SAN types:

- DNS
- IP
- Email
- UPN
- URI

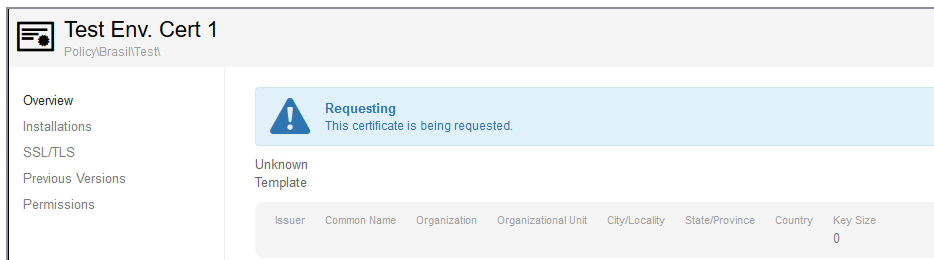
SAN types that are prohibited by policy do not appear on the screen.

To learn more about SANs, see ["About Subject Alternative Names \(SANs\)"](#) on page 174.

- b. Specify **Approvers** for the certificate's issuance.

- c. Choose Yes or No for the certificate's **Automatic Renewal**.
 - d. Use the list to select a **Certificate Authority**.
 - e. If requested, enter additional information required by the certificate authority.
4. Review the selection for **Start Processing on Creation**.
 This option has been automatically set based on your previous answers, so we recommend that you leave this setting alone. However, if you want to override the default action, you can do so, but know that it may mean previous settings in the wizard will not be honored.
 5. Click **Create Certificate**.
 You'll receive a confirmation that your certificate is being requested.
 6. If the Management Type is set to **Provisioning**, you will be prompted to add an installation now. If you want to add an installation, click **Yes, Add Installation**.

For information about adding an installation, see ["Creating a certificate installation" on page 476](#)



After the certificate is returned from the Certificate Authority (CA), if you've set up email notifications, the Contacts you've listed will receive a confirmation email.

For information on how long it takes for a certificate authority to act on a certificate request, and how Trust Protection Platform handles delays in certificate issuance, see ["How long does it take for a certificate authority \(CA\) to issue a certificate?" on page 451](#).

Choosing a key algorithm based on the certificate authority (CA)

When you request a new certificate you'll be asked to choose a key algorithm.

Use these tables to help you determine which key algorithm best suits your needs.

Certificate Authority	Notes
Adaptable CA	Supported
Sectigo Certificate Manager (SCM)	May require the addition of special account features. Contact the CA for help.
DigiCert CertCentral	Supported
Entrust Certificate Services	Requires a certificate product that supports ECC such as <i>Advantage</i> .
GlobalSign	Supported
HID PKIaaS	May require the addition of special account features. Contact the CA for help.
Microsoft Active Directory Certificate Services (ADCS) - Enterprise and Standalone	Requires a template that uses an EC algorithm name (Cryptography tab).
Open SSL	Supported
QuoVadis	May require the addition of special account features. Contact the CA for help.
RedHat Certificate System	May require special features that are not installed or licensed by default. Contact the CA for help.
RSA Certificate Manager	May require special features that are not installed or licensed by default. Contact the CA for help.
Self-signed	Supported
Symantec MPKI	Requires a certificate product that supports ECC such as <i>Premium</i> and an ECDSA signature algorithm specified on the CA template.
Verizon UniCERT	May require special features that are not installed or licensed by default. Contact the CA for help.

Amazon Certificate Manager

GeoTrust Reseller

VikingCloud

- If you selected **ECC**, select the **Elliptic Curve** name.
- If you selected **RSA**, select the **Key Strength**.

NOTE To see a comparison chart, see "About RSA and elliptic curve cryptography (ECC) key algorithms" on the next page.

Create a New Certificate

Folder | Certificate Signing Request | Additional Information | Submitted

Hash Algorithm
SHA-256

CSR Generation
Generate a CSR for me

Common Name* ?

Organization
Venafi

Organizational Units
Engineering x

City/Locality
SLC

State/Province
Utah

Country
US

Key Algorithm*
ECC
RSA
ECC
Previous

Cancel Next

Key Algorithm*
ECC

Elliptic Curve*
P256
P256
P384
P521

Cancel Next

About RSA and elliptic curve cryptography (ECC) key algorithms

RSA and ECC are two key algorithms. RSA is the most common; but ECC is gaining ground as an alternate, secure encryption method.

DID YOU KNOW? In RSA, the public key is a large number that is a product of two primes, plus a smaller number. The private key is a related number. In ECC, the public key is an equation for an elliptic curve and a point that lies on that curve. The private key is a number.

When you're deciding which algorithm to use for encryption, consider the following points:

- While in several respects, ECC is considered a viable option, some devices don't yet support ECC
- Trust Protection Platform supports the 3 **primary** NIST-supported ECC key strengths, and only supports NIST EC curves. For example, we *do* support PRIME256v1. We do *not* support SECP256k1.
- Both the Apache and CAPI drivers support ECC

NOTE ECC support using the Apache driver applies to SafeNet Luna SA only.

Comparing RSA and ECC key algorithms

- RSA is an asymmetric cryptographic algorithm used to encrypt and decrypt messages using public and private keys.
- ECC is an algorithmic alternative to RSA that can have computational benefits because its size is smaller but comparably stronger. ECC-enabled TLS can be faster and more scalable and provides the same or better security than the default cryptography that is currently in general use.

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA ²¹	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Taking action on a certificate

Certificates can be created, renewed, retired, deleted, replaced, and revoked.

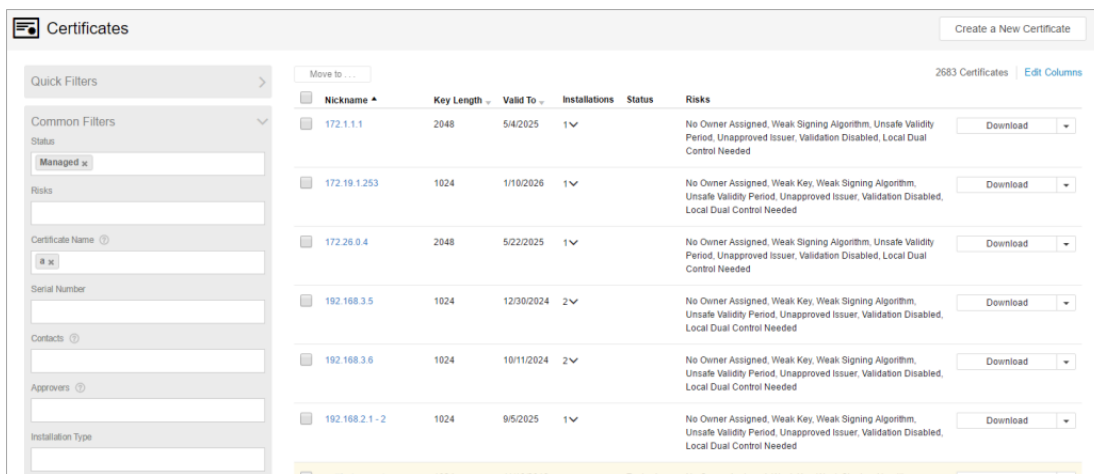
This chapter contains the following topics:

View an individual certificate's details, including certificate permissions and installations

You can view a certificate's details, including the certificate's locations and permissions.

To view a certificate's details

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. Use filters to help you find the certificate.
3. From the Certificates list, click the certificate's name.



Certificate Details Explained

Certificate details are grouped to make it easier for you to find and analyze relevant information. Use the tabs on the left to switch between sections. The sections on a certificate details page are:

- Overview
- Installations
- SSL/TLS
- Previous Versions
- Permissions

Overview

A certificate details Overview page might look like this:

VEN-25343
Policy\AA Aperture Policies\Myard's Test Folder\jared\

Pending My Approval
This certificate needs an approval in order to continue the renewal process.

Server Certificate Template

Issuer	Common Name	Organization	Organizational Unit	City/Locality	State/Province	Country	Key Size	Key Usage
VenQA CA	VEN-25343	Testing					2048	Digital Signature, Key Encipherment (a0)

Enhanced Key Usage
Server Authentication (1.3.6.1.5.5.7.3.1)

EXPIRATION
441 Days Left 11/9/2017
✓ Will Renew in 411 Days

SSL/TLS
Failed 8/25/2016 12:03 AM

Show All Properties

The **Actions** button in the upper-right corner allows you to take certain allowed actions on the certificate. The actions that are available depend on both the certificate status, as well as your account's permissions relative to the certificate. If no actions are available to you, that information will appear when you click the Actions button.

NOTE If Trust Protection Platform is creating the certificate naming request, the only Subject Alternative Name that is supported is DNS.

Click **Show all Properties** to see all the details.

Installations

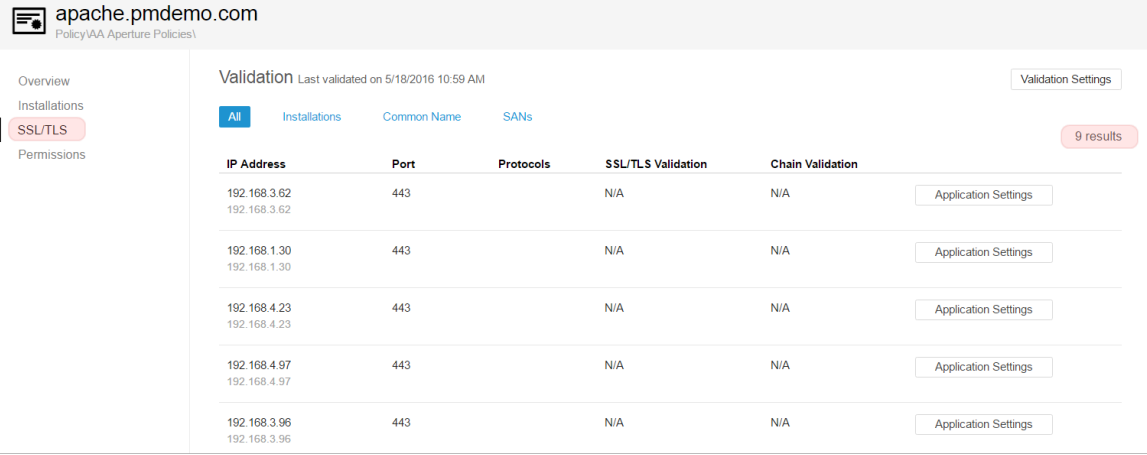
Click **Installations** in the sidebar to see a list of applications and devices on which the certificate is installed.

Installation Type	Device	Contacts	Installation Status	SSL/TLS Validation Port
App-444-test CAPI	192.168.3.98	local Dash3	Disabled	444
App-446 Basic	192.168.3.98	local Admin	Installation Validation Not Supported	446
App-447 Basic	192.168.3.98	local Admin	Installation Validation Not Supported	447
App-448 Basic	192.168.3.98	local Admin	Installation Validation Not Supported	448
App-449 Basic	192.168.3.98	local Admin	Installation Validation Not Supported	449

The action button on the right side of each row gives you the option to perform various actions on the installation. For more information on installations and the actions you can take, see [Certificate installations](#).

SSL/TLS

Click **SSL/TLS** to view validation information.



apache.pmdemo.com
Policy\AA Aperture Policies\

Overview
Installations
SSL/TLS
Permissions

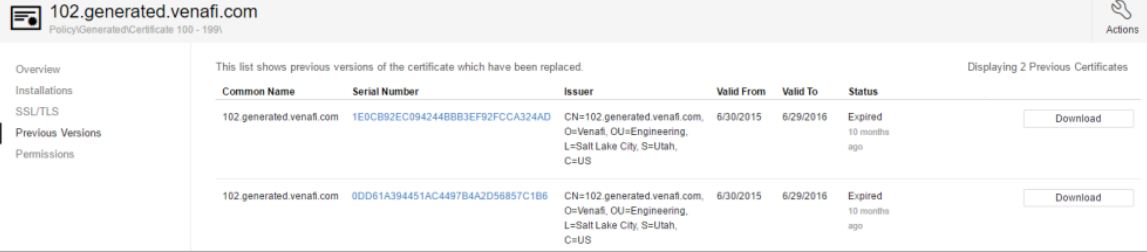
Validation Last validated on 5/18/2016 10:59 AM Validation Settings

All Installations Common Name SANs 9 results

IP Address	Port	Protocols	SSL/TLS Validation	Chain Validation	
192.168.3.62 192.168.3.62	443		N/A	N/A	Application Settings
192.168.1.30 192.168.1.30	443		N/A	N/A	Application Settings
192.168.4.23 192.168.4.23	443		N/A	N/A	Application Settings
192.168.4.97 192.168.4.97	443		N/A	N/A	Application Settings
192.168.3.96 192.168.3.96	443		N/A	N/A	Application Settings

Previous Versions

Sometimes you need to see historical data about a certificate, including older versions of a certificate. Click **Previous Versions** to see the common name, serial number, issuer, validity dates, status, and private key information of previous versions of the certificate.



102.generated.venafi.com
Policy\Generated\Certificate 100 - 199\

Overview
Installations
SSL/TLS
Previous Versions
Permissions

This list shows previous versions of the certificate which have been replaced. Displaying 2 Previous Certificates

Common Name	Serial Number	Issuer	Valid From	Valid To	Status	
102.generated.venafi.com	1E0CB92EC094244BBB3EF92FCCA324AD	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download
102.generated.venafi.com	0DD61A394451AC4497B4A2D56857C1B6	CN=102.generated.venafi.com, O=Venafi, OU=Engineering, L=Salt Lake City, S=Utah, C=US	6/30/2015	6/29/2016	Expired 10 months ago	Download

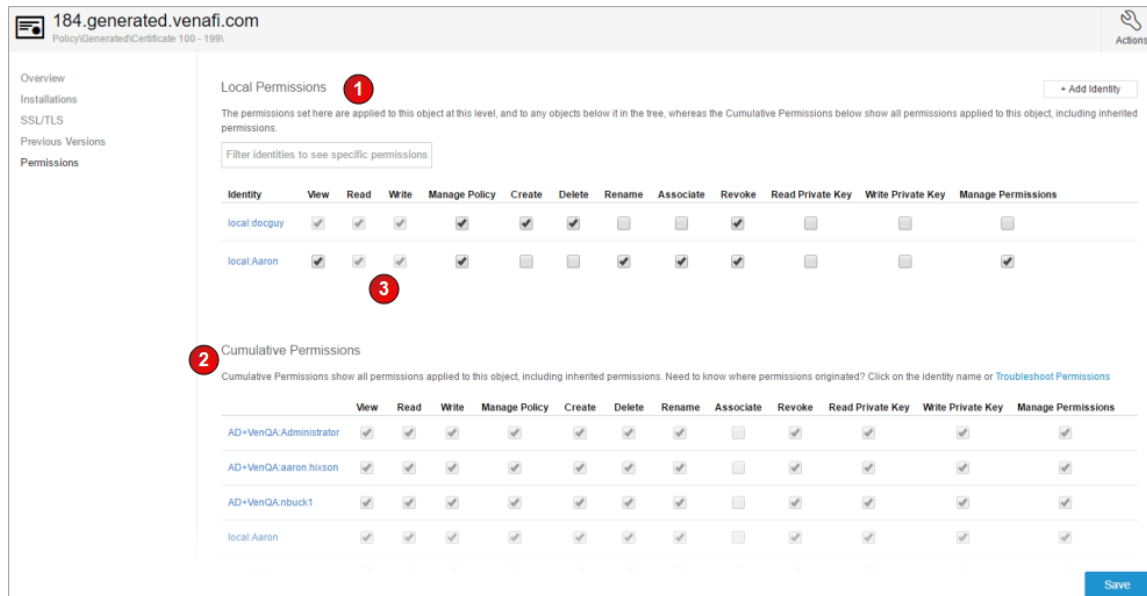
Click the serial number of a previous certificate version to see all historical data related to that version.

Click the **Download** button to download that version of the certificate to your local machine.

For more details, see "About Viewing Certificate History" on page 313.

Permissions

Click **Permissions** to set permissions on the certificate. To learn about permissions, see [Permissions overview](#).



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 in Aperture](#).

How long does it take for a certificate authority (CA) to issue a certificate?

Some certificate authorities can issue certificates almost instantly while others can take up to an hour or more to act on a CSR enrollment.

To prevent unnecessary resource utilization, and to avoid overloading the CA with repeated duplicate requests, Trust Protection Platform employs a system that periodically checks to see if the certificate has been issued. If the certificate has not been issued, the duration between requests gradually increases until it reaches 32 minutes.

By default, the retry interval period is 30 seconds, then 1 minute, 2 minutes, 4 minutes, 8 minutes, 16 minutes, and finally 32 minutes.

Once the duration reaches 32 minutes, the system will continue to check every 32 minutes until the certificate is issued. Therefore, the longer it takes the CA to approve the request, the longer it will take to import a certificate. For example, if it takes the CA a day to complete the request, it will take Trust Protection Platform up to 32 minutes after the certificate is issued to be imported into the system.

NOTE Some TPP drivers have a different retry interval period because the CA may return a certificate before the default 30 seconds. These CA templates and their intervals are:

Adaptable CA, Amazon CA (using private CA), and Google Private CA - 1 second, 2 seconds, 10 seconds, 30 seconds, 1 minute, 2 minutes, 4 minutes, 8 minutes, 16 minutes, then 32 minutes

Amazon CA (using public CA) - 10 minutes

VikingCloud - 30 minutes

You may wonder what are the primary causes of delays in certificate issuance?

There are several reasons why certificate issuance can be delayed:

1. The certificate authority is just slow. Some certificate authorities regularly take 30 minutes to an hour to act on a CSR.
2. Sometimes organizations have configured a CA approval for which a manual approval is required before a certificate can be approved. In those cases, the delay will be as long as it takes for the approver to receive and act on the request for approval.

NOTE This is completely outside the control of Trust Protection Platform. This is a setting controlled by the CA when approvals are required. If your organization is one that uses this type of setup, we encourage you to look at settings in Trust Protection Platform that perform the same function. These include Certificate Workflows and the Adaptable Workflow feature which can integrate with external approval systems, like, for example, ServiceNow where approvals can be managed.

For more information on certificate workflows, see ["Implementing certificate workflow management" on page 557](#).

For more information on Adaptable Workflow, see ["About Adaptable Workflows" on page 578](#).

3. Sometimes the certificate authority needs the customer to re-verify ownership of the domain before it will issue a certificate for the requested domain.

If Trust Protection Platform seems slow importing the certificate, the delay is likely on the certificate authority's side. Trust Protection Platform will continue checking every thirty minutes or so until the certificate is issued and can be imported into the system. If you have questions, check with your system administrator, or the person who administers manual approvals for your certificate authority.

Downloading certificates, private keys, and root chains

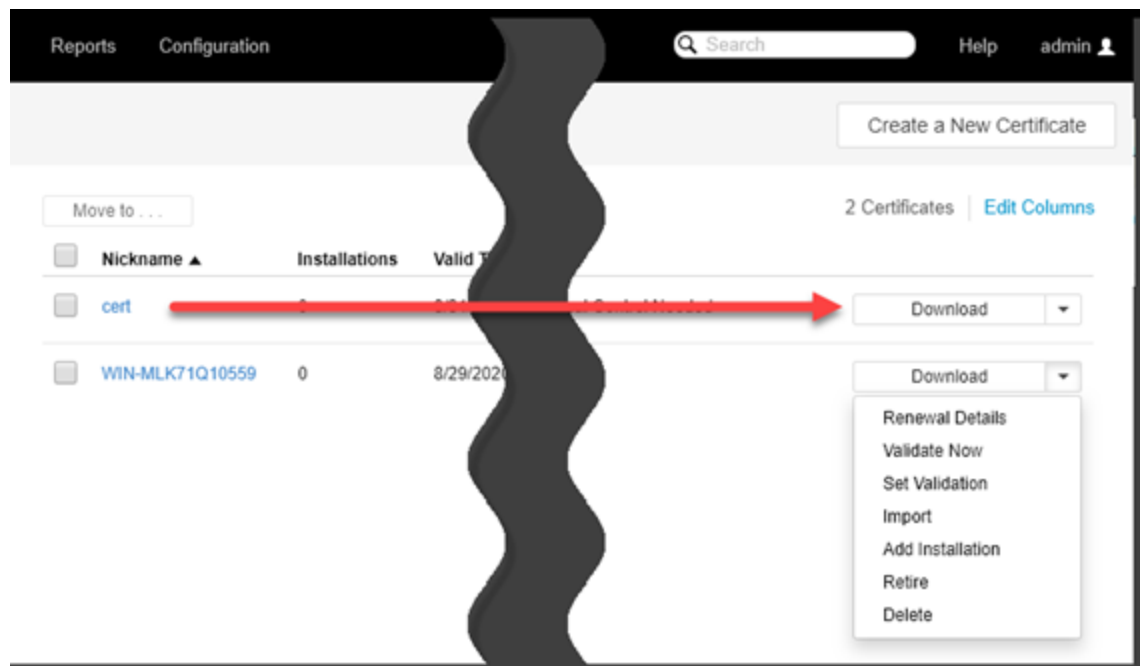
You can download the certificate, private key, and root chain from the Trust Protection Platform database so you can manually install them on your servers.

To download a certificate, private key, and root chain using Aperture

1. From the [TLS Protect](#) menu bar, click [Inventory](#) > [Certificates](#).

TIP You can also access the Download option from a specific certificate's **Details** page.

2. In the certificate list, find the certificate you want to download.
3. Choose one of the following:
 - From the certificate list, click **Download** using the action button.



-  Click the certificate's **Nickname** to open its details page, and then click **Actions** > **Download**.

4. From the **Format** list, select the format you want to use for the download.

- PEM (PKCS#8)
- PEM (OpenSSL)
- DER
- PKCS#7
- PKCS#12
- Java Keystore (JKS)

What if PKCS#12 isn't listed?

If PKCS#12 isn't listed it could be due to one or more of the following reasons:

- the user doesn't have *Private Key Read* permission
- the certificate doesn't have a private key
- the certificate was enrolled with a User Provided CSR
- the certificate was found during the Discovery process

PKCS#12 requires the private key to be available. If Trust Protection Platform does not have the private key or if the user does not have permissions to download the private key, PKCS#12 will not be a download option.

(Optional) If you select Base64 (OpenSSL) or PKCS#12 formats, you can configure the Friendly name, which will be used as the alias for the certificate.

(Optional) If you select PKCS#12 format, you can define a password. It will be required to access the downloaded certificate and private key.

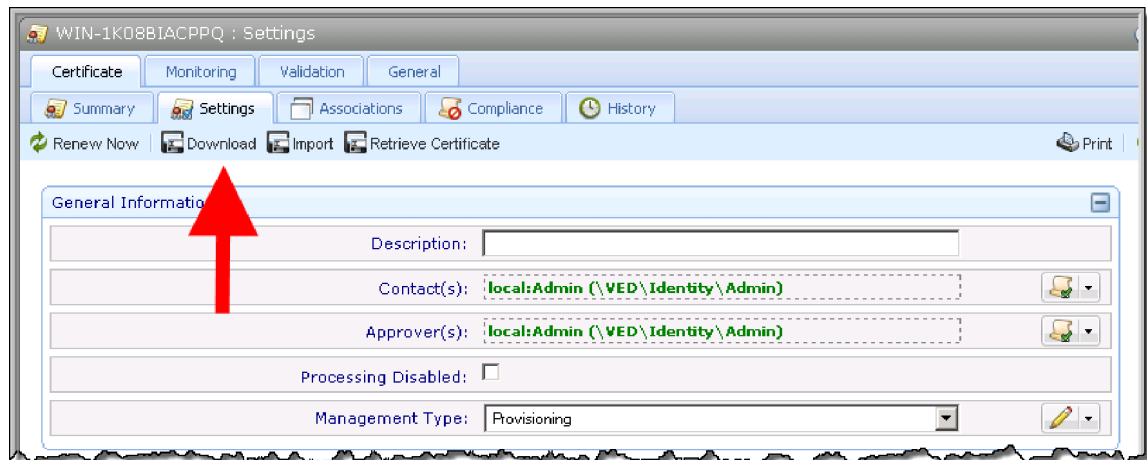
5. Enter names and passwords as needed.
6. Click **Download**.
7. Follow the onscreen prompts to download and install the certificate.

To manually download a certificate, private key, and root chain using Policy Tree

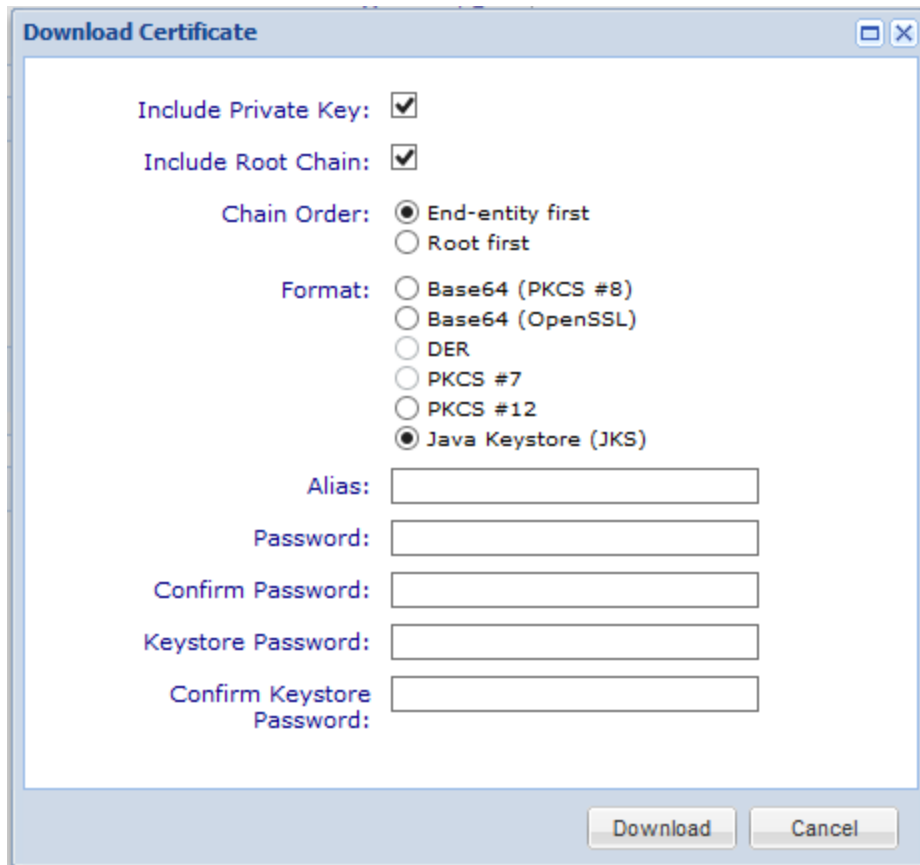
1. Log in to Policy Tree.

IMPORTANT You must have *view* and *read* permissions to the Certificate object to download the certificate or root chain. You must have the *private key read* permission to the Certificate object to download a private key.

2. From the Tree drop-down menu, select the **Policy** tree.
3. In the Policy tree, select the Certificate object from which you are going to download the certificate and private key.
4. Do one of the following:
 1. Click the **Certificate > Settings** tab.
 2. Click the **Certificate > History** tab.
 3. Click  **Download**.



5. The Download Certificate dialog appears.

A screenshot of a 'Download Certificate' dialog box. The dialog has a title bar with a maximize button and a close button. Inside, there are several options: 'Include Private Key' and 'Include Root Chain' are both checked with checkboxes. 'Chain Order' has two radio buttons: 'End-entity first' (selected) and 'Root first'. 'Format' has six radio buttons: 'Base64 (PKCS #8)', 'Base64 (OpenSSL)', 'DER', 'PKCS #7', 'PKCS #12', and 'Java Keystore (JKS)' (selected). Below these are five text input fields labeled 'Alias:', 'Password:', 'Confirm Password:', 'Keystore Password:', and 'Confirm Keystore Password:'. At the bottom right are 'Download' and 'Cancel' buttons.

Download Certificate

Include Private Key: ☒

Include Root Chain: ☒

Chain Order: ☒ End-entity first
☐ Root first

Format: ☐ Base64 (PKCS #8)
☐ Base64 (OpenSSL)
☐ DER
☐ PKCS #7
☐ PKCS #12
☒ Java Keystore (JKS)

Alias:

Password:

Confirm Password:

Keystore Password:

Confirm Keystore Password:

Download Cancel

6. (Optional) To include the private key with the certificate download, select **Include Private Key**.
7. (Optional) To include the certificate's associated root and intermediate root certificates, select **Include Root Chain**.
8. Designate the format in which you want to save the certificate files.
 - Base64 (PKCS#8)
 - Base64 (OpenSSL)
 - DER
 - PKCS#7
 - PKCS#12
 - Java Keystore (JKS)

What if PKCS#12 isn't listed?

If PKCS#12 isn't listed it could be due to one or more of the following reasons:

- the user doesn't have *Private Key Read* permission
- the certificate doesn't have a private key
- the certificate was enrolled with a User Provided CSR
- the certificate was found during the Discovery process

PKCS#12 requires the private key to be available. If Trust Protection Platform does not have the private key or if the user does not have permissions to download the private key, PKCS#12 will not be a download option.

(Optional) If you select the Base64 (OpenSSL) or PKCS#12 formats, you can configure the Friendly name, which will be used as the alias for the certificate.

(Optional) If you select PKCS#12 format, you can define a password. It will be required to access the downloaded certificate and private key.

9. Click **Download**.
10. In the File Download dialog, click **Save**, then browse to the Directory where you want to save the file.
11. Click **Save** to save the file.

Trust Protection Platform downloads the certificate and, optionally, the private key and root chain, from the Trust Protection Platform database. You can now use the download file to install the certificate, private key, and root chain on your encryption system servers.

Extracting and downloading PEM contents into separate files

You can avoid having to manually extract PEM contents—the sections that contain the private key and root chain—following a certificate download. Trust Protection Platform can do that for you and then package them up into a zip file for downloading.

When you enable the *Extract PEM content into separate files* option, the resulting download appears as a single zip file that contains certificate, key and root chain files (depending on which ones you specify):

- Certificate (.crt)
- (Optional) Chain Certificates (-chain.pem)

- (Optional) Private Key (.key)

Root chains are included in the zip file in two ways:

- As individual PEM files, one for each CA certificate, and
- As a single PEM formatted chain bundle file that includes all of the CA certificates concatenated together in the *chain order* that you specify and without any extra comments or text.

The file name is based on the CN of the certificate with *-chain.pem* added as the *suffix.file_* extension.

NOTE The chain does not include the subject/issuer informational headers that are included when the certificate and chain are downloaded together in the same PEM file.

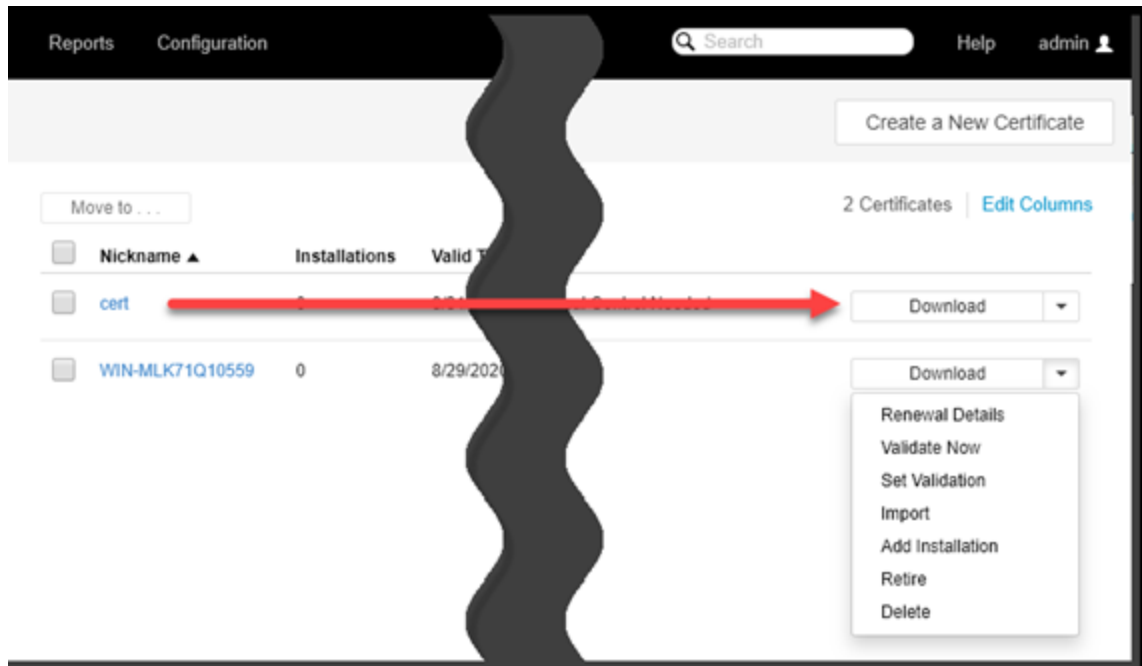
To extract and download PEM contents as separated files

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.

TIP You can also access the Download option from a specific certificate's **Details** page.

2. In the certificate list, find the certificate you want to download.
3. Choose one of the following:

- From the certificate list, click **Download** using the action button.



- Click the certificate's **Nickname** to open its details page, and then click **Actions** > **Download**.
- In the **Download** box, click **Format** and select one of the available PEM formats from the list.
 - PEM (PKCS#8)
 - PEM (OpenSSL)
 - (Optional) Select one or both of the following components to include in the download:
 - Root Chain**
 - Private Key**
 - (Conditional) If you selected *Root Chain* in the previous step, then specify the order in which you want all of the concatenated CA certificates included by selecting either **End Entity First** or **Root First** from the **Chain Order** list.
 - In the **Password** field, type a new password (and then type it again in the **Confirm Password** field to verify).

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
8. Select the **Extract PEM content into separate files** check box, and then click **Download**.

Configuring validation for certificates

You can configure certificate validation in TLS Protect. As part of validation, you need to specify the certificate's validation settings so that Trust Protection Platform can locate the certificate and verify that it's installed correctly.

IMPORTANT You must have *View* and *Write* permissions to the application.

To configure certificate validation

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. Find the certificate that you want to configure, and then click the certificate's name.
3. In the sidebar, click **SSL/TLS**.
4. Click **Certificate Settings**.
5. Edit the **Certificate SSL/TLS Validation Settings** as needed.

What each setting means

- **Validate SSL/TLS connections for this certificate?** Select **Yes** or **No**. Yes will enable Trust Protection Platform to turn on daily TLS validation of this certificate. The **Port** is the network port that Trust Protection Platform will use to connect to the target device hosting the certificate when making the TLS connection.
- **Use certificate's Common Name** - Validation scans include network addresses resolved from the common name of the certificate.

- **Use Certificate DNS Subject Alternative Names** - Validation scans include network addresses resolved from the DNS Subject Alternative Names (SANs) of the certificate, if any.
- **Validate the chain returned by the hosting server** - The chain returned by the hosting server is compared to the chain that Trust Protection Platform builds using its internal algorithm to ensure a match. By default, chain validation is enabled and affects the SSL/TLS validation result.
- You can define other network addresses and ports by creating a device and Basic application object.

See [Creating a device object in Policy Tree](#).

Renewing a certificate manually

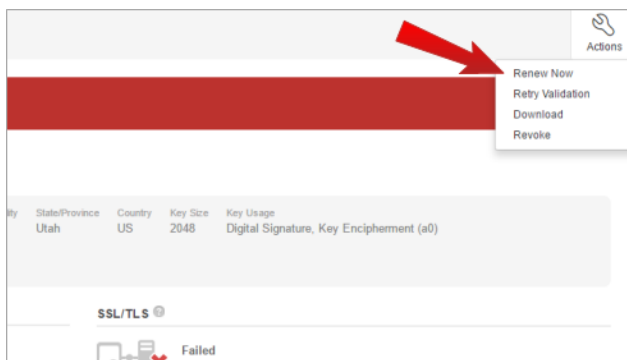
The Renew Certificate wizard walks you through identifying the certificate and specifying its location.

To renew a certificate

1. Find the certificate you want to renew.
2. You can use filters to help narrow your search.
3. In the certificate list, click **Renew Now** or in the certificate's detail page, click **Actions > Renew Now**.

The screenshot shows the 'Certificates' management page. On the left, there are 'Quick Filters' for Status (Expired - Short Term, Managed), Certificate Name, Serial Number, Contacts, and Approvers. The main table lists certificates with columns: Nickname, Installations, Valid To, Key Length, and Status. The certificate '2AMUTC.nb.venafi.com' is highlighted, and a red arrow points to the 'Renew Now' button in its status column. Other certificates listed include '* dontheadummy.org', '* venqa.venafi.com - 2', and '* venqa.venafi.com - 3'.

Nickname	Installations	Valid To	Key Length	Status	Action
- 1	0	2/12/2016	2048	Invalid Domain Name, In Error, Expired - Short Term, Failed Validation, Unapproved Issuer, Local Dual Control Needed	Retry Renewal
2AMUTC.nb.venafi.com	0	8/29/2016	2048	Expired - Short Term, Failed Validation, No Owner Assigned, Unapproved Issuer, Local Dual Control Needed	Renew Now
* dontheadummy.org	0	2/29/2016	2048	In Error, Expired - Short Term, No Owner Assigned, Local Dual Control Needed	Retry Renewal
* venqa.venafi.com - 2	1	3/9/2016	2048	Expired - Short Term, Failed Validation, No Owner Assigned, Unapproved Issuer, Local Dual Control Needed	Retry Validation
* venqa.venafi.com - 3	1	3/9/2016	2048	In Error, Expired - Short Term, Failed Validation, No Owner Assigned, Unapproved Issuer, Revoked, Local Dual Control Needed	Retry Renewal



4. Review the **Requested Renewal Details**.

Requested Renewal Details

CERTIFICATE REQUEST DETAILS

Certificate Folder	Policy\North America
Nickname	cert-100-1024-SHA1-RSA-42-3
Management Type	Provisioning
Contacts	admin
Hash Algorithm	SHA-256
CSR Generation	Generate a CSR for me
Common Name	cert-100-1024-SHA1-RSA-42-3
Organization	Venafi
Key Strength	2048
Approvers	admin
Automatic Renewal?	No
Certificate Authority	Policy\North America\Eng\MCSA

Edit and Renew

Cancel

Renew

5. Do one of the following:

- If no changes are needed, click **Renew**.
- If you need to make changes, click **Edit**, and then edit the Renewal Details.
- When you're done, click **Submit**.

In the certificate list, the state changes to **Renewing**.

Revoking a certificate

You can revoke a certificate from the certificate inventory or the certificate details page.

Move to ...		1410 Certificates Edit Columns					
☐ Nickname ▾	Installations	Valid To ▾	Key Size ▾	Status	Last Renewed By	Valid From ▾	
☐ root agency	4 ▾	12/31/2039	512			5/28/1996	Download ▾
☐ fw.venafi.net.au	1 ▾	12/31/2037	2048			11/12/2015	Download ▾
☐ microsoft root authority	4 ▾	12/31/2020	2048			1/10/1997	Download ▾
☐ wmsvc-win-1k08biacppq	1 ▾	10/9/2020	2048			10/12/2010	Download ▾
☐ vdi-dev-dir-11	0	6/18/2020	1024			6/19/2015	Download ▾
☐ Duplicate 1	1 ▾	8/11/2019	2048			12/15/2016	Download ▾
☐ *.lds.org	1 ▾	4/17/2019	2048	Failed Revocation		1/9/2017	Retry Revocation ▾
☐ DESKTOP-19D7ARV	0	4/20/2018	2048			4/20/2017	Download ▾
☐ sctestlab.venafi.com	1 ▾	3/14/2018	2048			3/14/2016	Download ▾
☐ 102.generated.venafi.com	23 ▾	2/6/2018	2048			12/7/2014	Download ▾
☐ Jared-PC	0	12/5/2017	2048			12/5/2016	Download ▾
☐ ahixson-dir1	0	12/1/2017	2048			12/1/2016	Download ▾
☐ ahixson-dir1a	0	12/1/2017	2048			12/1/2016	Download ▾

BEST PRACTICE It's a good idea to revoke certain certificates to prevent security breaches. For example, if an employee transfers to another department or leaves the company and has access to private key information for certain certificates, you should revoke those certificates and replace them.

To revoke a certificate

1. From the certificate list for the user you searched for, find the certificate you want to revoke.
2. Do one of the following:
 - From the certificate inventory, click **Revoke** on the action button.
 - From the certificate details page, click **Actions > Revoke**.
3. From the **Reason for Revocation** list, select a reason.

4. Click **Revoke** but remember, *this action cannot be undone*.

Revoke

Revoking this certificate will make it invalid. This action cannot be undone. If you decide later that the certificate is still needed, you will need to renew the certificate to request a new version that can be used.

Reason for Revocation
Unspecified

Comment

Common Name	Aaron Hixson
Organization	Venafi, Inc.
Organizational Units	Engineering
City/Locality	Salt Lake
State/Province	Utah
Country	US
Hash Algorithm	SHA-1
Has Private Key	Yes

Cancel Revoke

NOTE Revoking a certificate makes it invalid. The Certificate Authority is notified of this action.

Resolving problems for Revocations that resulted in a processing error

Revocations can fail for a number of reasons. The most common reasons revocations fail include:

- The revocation request was rejected by an approver
- The credentials to authenticate to the Certificate Authority were wrong
- Trust Protection Platform did not have the appropriate CA template configured for the CA that the certificate was issued from.

You can review the error message that will tell you why the revocation failed.

When Revocation fails, you have two choices:

- **Cancel.** Canceling a revocation means that even though it failed, you do not intend to retry revocation and you simply wish to clear the processing error from Trust Protection Platform. For example, you would do this in situations where the approver has rejected your request to revoke the certificate and you don't expect to receive approval on subsequent requests.
- **Retry.** Retry will clear the error and attempt revocation again. You should only do this after you have resolved the problem that caused the error in the first place. For example, if the revocation failed because the Certificate Authority credentials expired, you will need to ask your Administrator to update the credentials before you attempt revocation again. If it failed because it was rejected by approval, you will need to review the rejection reasons and retry after the approver's requirements have been met.

Checking revocation status of a certificate

If you have requested to have a certificate revoked, or if you just want to verify a certificate has not been revoked, you can use the Check Revocation action on the certificate to verify its revocation status. When you check the revocations status of a certificate, Trust Protection Platform uses OCSP to contact the Certificate Authority and check the status of that certificate. If it cannot verify the status via OCSP, the system will check the Certificate Revocation List (CRL) for that CA to see if the certificate has been published as being revoked by the CA. The Revocation Checking section of the Certificate Details screen will show the status of the revocation check.

To check the revocation status of a certificate

1. Open the Certificate Inventory.
2. Locate the certificate you want to check.
3. Do one of the following:
 - a. From the certificate inventory, click **Check Revocation** on the action button.
You will need to open the Certificate Details page to see the results of the revocation status check.
 - b. From the certificate details page, click **Actions > Check Revocation**.
4. On the Certificate Details page, look at the Revocation Checking section to see the status.
You may need to refresh your browser to see this section update.

For more information about revoking a certificate, see ["Revoking a certificate" on page 463](#).

Retiring a certificate

At the end of a certificate's lifecycle, you should retire it. If you don't retire certificates, you'll continue to receive notifications, warnings, and renewal notices.

The Retire action is available to a user under the following conditions:

- User must have `View/Write` permissions to the certificate.
- Certificate must meet all of the following states:

- NOT already Retired/Disabled
- NOT in error
- NOT currently processing (for example: renewing, installing, or revoking)

To retire or disable a certificate

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Locate the certificate you want to retire.
3. Do one of the following:
 - From a row on the certificate inventory, click the action button, then click **Retire**.
 - From the certificate details page, click **Actions > Retire**.
4. Confirm that you want to retire the certificate by clicking **Yes, Retire**.

TLS Protect confirms that the certificate has been retired.



You can reactivate a retired certificate. To learn how, see "[Reactivating a retired certificate](#)" below.

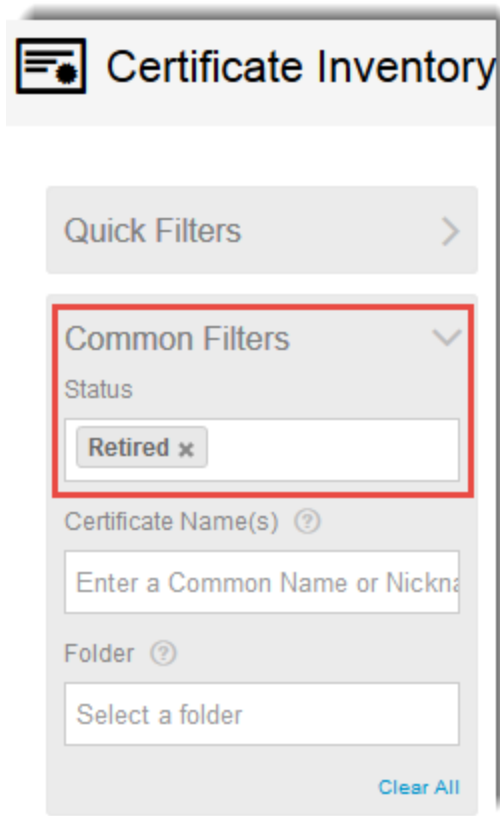
Reactivating a retired certificate

If you want to enable a retired certificate, you can reactivate it. This situation might occur if a certificate was disabled or retired accidentally. However, once the certificate is revoked, you must get a new certificate because the Certificate Authority will revoke it and add it to the CRL (Certificate Revocation List).

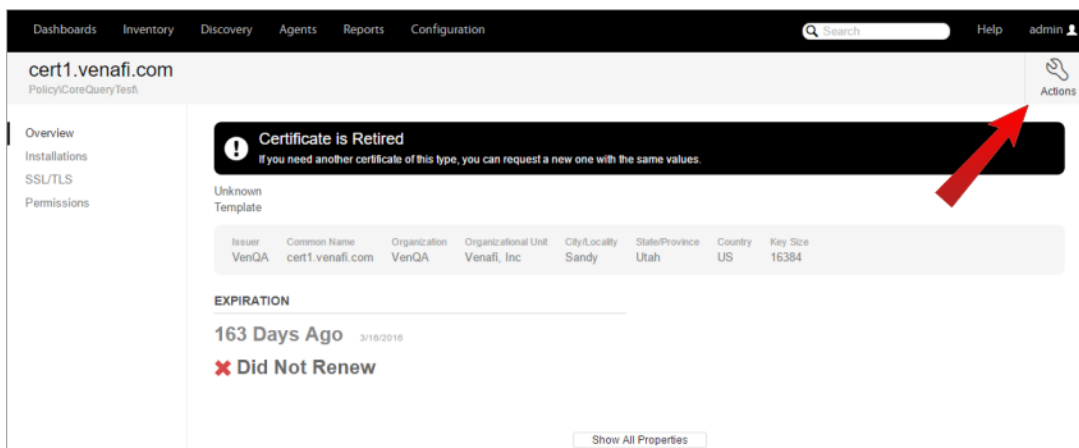
For more information about CRL's, see "[Understanding CRLs and CDPs](#)" on page 238.

To reactivate a retired certificate

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. In Common Filters, click the Status field and choose **Retired**.



3. In the certificate list, find the certificate that you want to reactivate.
4. On the certificate details page, click the Actions button, and then click **Reactivate**.



5. The certificate is returned to a **Managed** status with all of the settings that it had before it was retired.

Scheduling a certificate renewal

You can schedule certificate renewals to ensure a critical certificate doesn't expire, which could result in an outage.

To schedule a certificate renewal

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.

Nickname	Key Length	Valid To	Installations	Status	Risks	Actions
172.1.1.1	2048	5/4/2025	1	✓	No Owner Assigned, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download
172.19.1.253	1024	1/10/2026	1	✓	No Owner Assigned, Weak Key, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download
172.26.0.4	2048	5/22/2025	1	✓	No Owner Assigned, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download
192.168.3.5	1024	12/30/2024	2	✓	No Owner Assigned, Weak Key, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download
192.168.3.6	1024	10/11/2024	2	✓	No Owner Assigned, Weak Key, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download
192.168.2.1-2	1024	9/5/2025	1	✓	No Owner Assigned, Weak Key, Weak Signing Algorithm, Unsafe Validity Period, Unapproved Issuer, Validation Disabled, Local Dual Control Needed	Download

2. Locate the certificate you want to modify, and then click its nickname to open the certificate details page.
3. Click the **Actions** button, and then click **Renewal Schedule** or **Renewal Details**.

Validation Failed
There was an error during validation. Check the validation results for the specific error message.

Server Certificate
Template
45 Day Cert

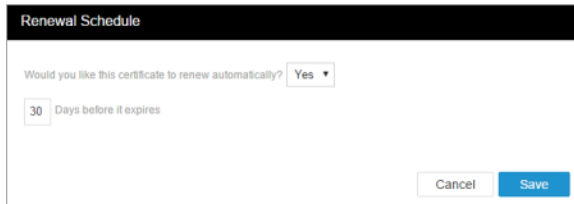
Issuer	Common Name	Organization	Organizational Unit	City/Locality	State/Province	Country	Key Size	Key Usage
VenQA CA	*test.venafi.com		Testing				2048	Digital Signature, Key Encipherment (a0)

Enhanced Key Usage
Server Authentication (1.3.6.1.5.5.7.3.1)

EXPIRATION
41 Days Left 10/6/2016
✓ Will Renew in 11 Days

SSL/TLS
Failed
8/25/2016 12:04 AM

4. Set the renewal details, and then click **Save**.



Renewal Schedule

Would you like this certificate to renew automatically? Yes ▾

30 Days before it expires

Cancel Save

Resolving certificate errors

When a certificate is in an errored state you will see a warning banner at the top of the Certificate details page.

There are many reasons why a certificate might be in error. For example, maybe the Certificate Authority template may have been misconfigured, or the certificate authority server may have been down. Once the underlying issue is resolved, you can use TLS Protect to continue the process. In general, you will be able to take action on an errored certificate if your user account has the following permissions:

- View
- Write

There are several ways to resolve the error, depending on the specific error.



Renewal Error
Missing Certificate Authority, unable to process

Server Certificate
Template
TimWeb

Issuer	Common Name	Organization	Organizational Unit	City/Locality	State/Province	Country	Key Size	Key Usage
VenQA CA	*.dontbeadummy.org	Venafi, Inc	QA	Sandy	Utah	US	2048	Digital Signature, Key Encipherment (a0)

On the first line of the banner, you see the type of error. Error types include:

- Renewal Error
- Enrollment Error
- Installation Error
- Revoked

The second line shows the specific error message. This information will help you determine how to proceed.

The steps to correct the error depend on whether the error is due to an issue within a certificate or not. Two typical actions to resolve issues are:

- **Cancel the request.** If you need to make changes to the request itself, either because information is missing or is invalid, you must cancel the process, fix the issue, then resubmit the request.

For example, you may need to provide a missing certificate authority, fix a duplicate private key, etc. Once you have addressed the underlying data problem, you will resubmit the request which will also kick off any necessary approvals.

- **Retry the request.** If the problem encountered was temporary in nature, and not related to the data in the request, you have the option to retry the request. :

Some errors are not data problems. For example, you may have experienced a network outage, or the certificate authority may have been unavailable when the original request was processed. In these cases, where no data change is necessary, you can simply retry the request after the issue is resolved.

EXAMPLE In the image above, the specific error message is "Missing Certificate Authority, unable to process." To resolve this error, you would click **Actions > Cancel the Renewal**, then open the certificate and add a certificate authority, then start the renewal process again by clicking **Actions > Renew Now**.

The Action button allows you to easily attempt to resolve the issue. The action button options will depend on the type of current process that was being attempted, and will change, depending on the specific error message, as well as your account's permissions relative to the certificate.

If you click the cancel action, a window shows information related to what will happen if you cancel the pending action. You must click **Yes, Cancel Request** to finalize the action.

Renaming a certificate

You may decide that you want to change the nickname associated with a certificate to make it easier to locate, or make the name more user friendly or meaningful. You can rename a certificate on the certificate details page in Aperture.

To rename a Certificate

NOTE You need the **rename** permission to the certificate, or this functionality won't be available to you.

1. From the SSH Protect menu bar, click **Inventory** , and then click **Certificates**.
2. Locate the certificate you want to change.
3. Click on the certificate name to open the details page.
4. Hover your mouse pointer over the certificate name until you see the name highlighted, and then click it.
5. In the **Rename** box, type the new name in the **New Name** field, and then click **OK**.

Object names may not contain the backslash \ or less-than sign < characters. Object names (including their path ancestors in the policy tree) must be fewer than 255 total characters.

Deleting a certificate

If you want to stop tracking a certificate, and you want to remove all information about the certificate, you can delete a certificate. You delete a certificate on the certificate details page.

Usually at the end of a certificate's lifecycle you will want to *retire* a certificate, rather than delete it. Deleting a certificate completely removes the certificate from the system including all historical information associated with the certificate. For information on retiring a certificate, see "[Retiring a certificate](#)" on [page 465](#).

An example of a certificate you might want to delete is a certificate that was created in error, or one created for testing purposes.

To delete a certificate

1. Locate the certificate that you want to delete in the certificate inventory, and open it to see the certificate details page.
2. Click the **Action** button, and then click **Delete**.

You will not see the Delete link if your account doesn't have permission to delete the certificate.

3. The system checks to see if there are installations associated with the certificate, and if so, what your permissions are on those related installations.

- If there are no installations associated with the certificate, a modal confirmation appears warning you that the delete action cannot be undone.
- If there are installations associated with the certificate, the system won't let you orphan the installations. To ensure the installations are not orphaned, TLS Protect checks to see what permissions you have for the associated installations.

The following table shows the combination of permissions that are checked on the installations tied to the certificate you want to delete, and what action you can take, based on your permissions on the installations.

Delete	Write or Associate	Action
Yes	No	You can delete all installations associated with a certificate, but you cannot reassign them to another certificate.
Yes	Yes	You can choose to delete all installations associated with a certificate, or you can reassign them to another certificate.
No	No	You cannot delete the certificate because you cannot edit the associated installations. Trust Protection Platform will not allow you to orphan installations.
No	Yes	You must re-assign all installations to another certificate.

If there are multiple installations tied to the certificate, then the action you can take applies to *all installations*. For example, if you have two installations, and you have delete permissions for one installation, but not the other, the system treats your permissions as if you do not have delete permissions.

If you want to take separate actions on the installations, you need to do that before you attempt to delete the certificate.

Moving certificates and keys in bulk after Discovery

After a discovery job is complete and certificates and keys have been placed, you may want to move items in bulk from one policy to another. This is especially helpful when moving certificates or keys from the default policy to their correct folders.

To move multiple certificates or keys at the same time (bulk move)

1. From the menu, open the correct inventory.
2. Select the items you want to move . You can use the filters to help you refine the list.
3. **Tip:** If you want to move all of the visible items, select the checkbox next to **Nickname**.

Move to ... 100 certificate(s) selected.

☒	Nickname	Installations	Valid To	Risks	Issuer
☒	101.generated			Failed Validation, No Owner Assigned, Unapproved Issuer	Google In
☒	102.generated.venafi.com	23	1/7/2019	Failed Validation, No Owner Assigned, Unapproved Issuer	QA Venafi
☒	103.generated.venafi.com	2	11/14/2018	Failed Validation, No Owner Assigned, Unapproved Issuer	QA Venafi
☒	104.generated.venafi.com	0	6/29/2016	No Owner Assigned, Weak Key	Self Signe
☒	105.generated.venafi.com	0	5/5/2018	No Owner Assigned, Unapproved Issuer	GlobalSig GlobalSig
☒	106.generated.venafi.com	0	11/13/2018	No Owner Assigned, Unapproved Issuer	QA Venafi

IMPORTANT The select all box only selects the visible items in the list. Thus, if there are 200 items that match the filter results, but only 100 items are displayed, on the 100 displayed items will be moved. To display more items, scroll to the bottom of the list and click the **Load** banner .

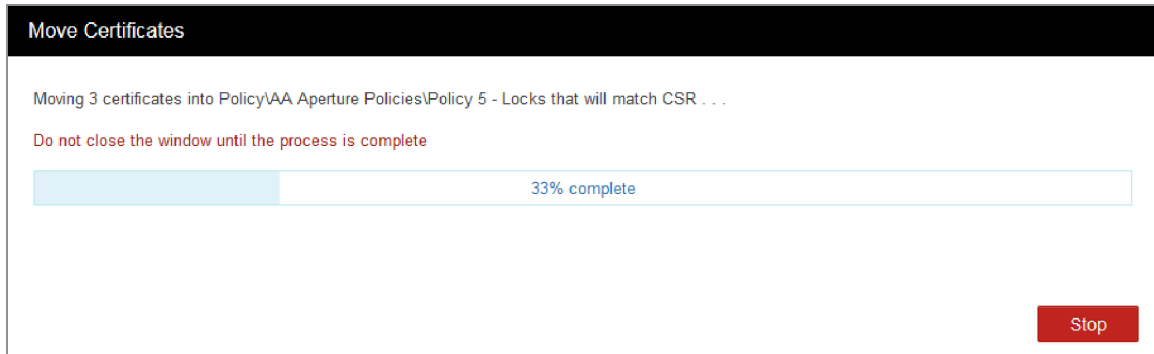
4. When you've selected the items you want to move , click **Move To...**

Move to ... 3 certificate(s) selected.

☒	Nickname	Installations	Valid To	Risks
☒	101.generated.venafi.com	1	12/19/2017	Failed Validation, No Owner Assigned, Unapproved Issuer
☐	102.generated.venafi.com	23	1/7/2019	Failed Validation, No Owner Assigned, Unapproved Issuer
☒	103.generated.venafi.com	2	11/14/2018	Failed Validation, No Owner Assigned, Unapproved Issuer
☐	104.generated.venafi.com	0	6/29/2016	No Owner Assigned, Weak Key
☒	105.generated.venafi.com	0	5/5/2018	No Owner Assigned, Unapproved Issuer

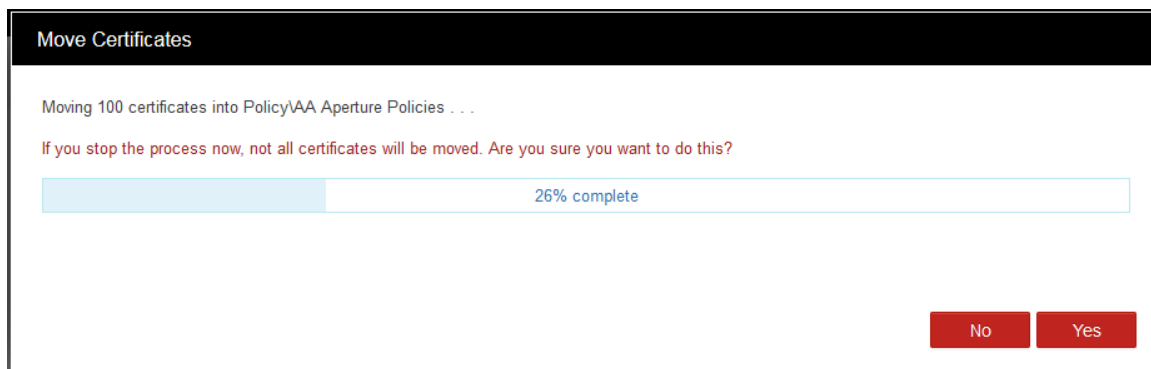
5. Use the drop-down arrow to choose the new folder.
6. Click **OK**.

You'll see a confirmation message and a progress bar indicating that items are being moved.



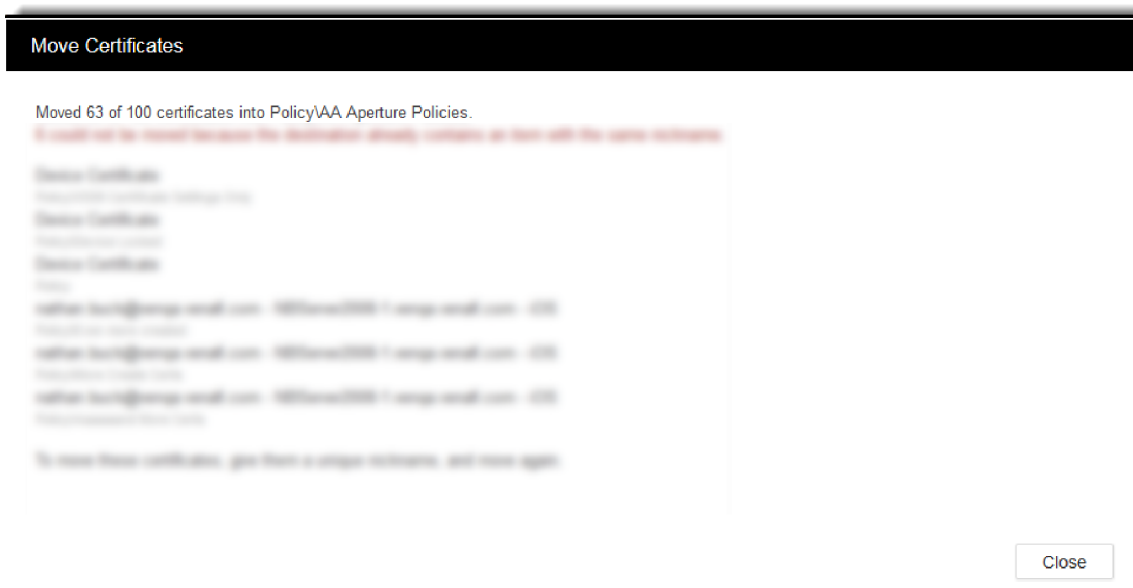
What if I need to stop the process?

1. To stop the move, click **Stop**.
2. Confirm that you want to stop the move by clicking **Yes**. If you want to continue the move, click **No**.



IMPORTANT If you stop the process, the certificates or keys that have already been moved will remain in their new folder.

3. Review the notification that tells you how many certificates or keys were moved before the stop was initiated.



Working with certificate installations

Installations are used to track where certificates are installed and automate the rotation of certificates when they are renewed. You can edit these installation settings and other metadata for tracking purposes.

NOTE In the Policy Tree, installations are called *application objects* or *applications*.

This chapter contains the following topics:

Creating certificate installations (applications)

You can create a certificate on its own but if you want to provision (automatically renew and install) it, you need to create and associate an application object for that certificate.

In the Policy Tree, there are two ways that certificate installations can be created, either using discovery, or by manually creating the installation in Policy Tree, where they are called *applications*.

For more information on creating certificate installations (applications) in Policy Tree, see [Creating an application](#).

In TLS Protect you can add an installation on the certificate inventory list, or via a quick action on the certificate details page. For more information see "[Creating a certificate installation](#)" below.

Creating a certificate installation

It is important to track where certificates are installed. You can leverage Trust Protection Platform to manually track where certificates are installed, set up automatic daily validation, or even have Trust Protection Platform automatically install the certificate for you on the target device.

You perform these tasks by adding an installation. You might choose to add an installation for every instance of a certificate you have deployed upon an environment. If you have, or want to have a certificate installed to five places, then you would add five installations in TLS Protect.

DID YOU KNOW? If you want an Entrust nShield HSM to secure private keys for your Apache HTTP servers, you can create multiple installations. When you create two or more installations for the same certificate, an Application Group appears in the Policy Tree. The Application Group is a set of Application objects that share the same certificate. You can only view and edit Application Groups in the Policy Tree. However, deleting an Application Group is not advisable.

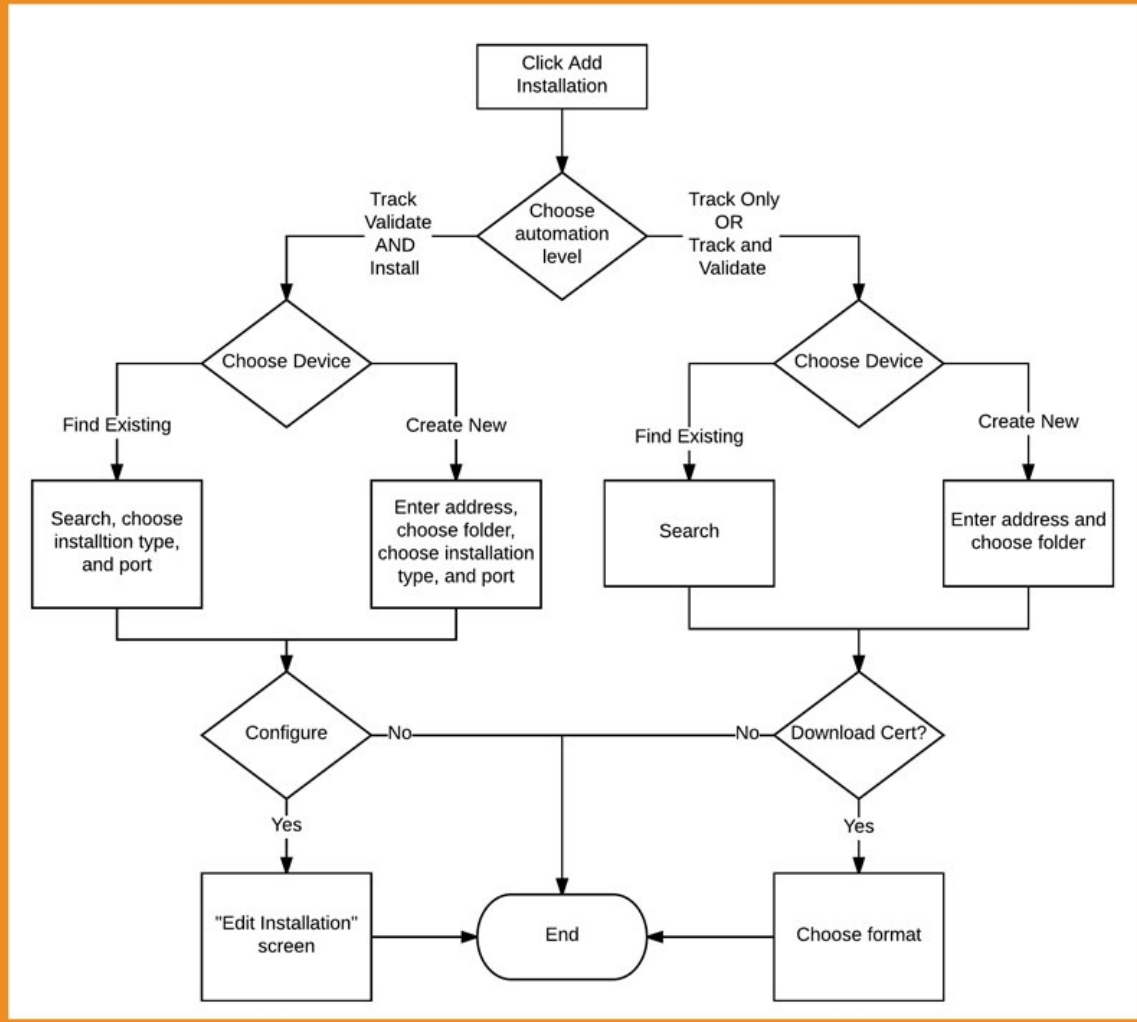
You can use the Add Installation wizard to create an installation for a certificate on a specific device. The wizard is *not* available for any of the following reasons:

- The certificate state is *Lost*, *In Error*, or *Retired*.
- The certificate management type is *Unassigned*.

NOTE You must have *view*, *read*, and *write* permissions to the certificate and you must have *create* and *write* permissions on the target device.

Flow-chart of certificate installation options

Create an Installation for a Certificate



To add an installation to a certificate

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. Using the filters, locate the certificate that has a Provisioning management type.
For more information, see ["Finding assets using filters on the Certificate Inventory list"](#) on page 400.
3. On the inventory list, use the quick action in the drop-down box, and click **Add Installation**.

You can create more than one installation for the same certificate.

CAUTION When you create the second installation for an Apache HTTP server and an Entrust nShield HSM manages the certificate, an Application Group appears in Policy Tree.

Although Application Groups are automatically created and managed in Aperture, they are only visible in the Policy Tree Policy tree. To avoid unexpected results in Policy Tree, do not delete Application Groups.

4. In the **Add a New Installation** wizard, select the method to track and manage the certificate, and then click **Next**. The options on subsequent screens depend on the tracking level you select:
 - **Track this certificate.** Use this option to manually download and install the certificate on a device. Venafi helps you track certificate renewal.
 - **Track and validate this certificate.** Use this option to allow daily certificate confirmation. If the certificate is absent on the device, you download and install it once. After that, each day, Venafi will use the hostname and port to connect and validate that the correct certificate version is available.
 - **Track, validate, and automate installation of this certificate.** Use this option to automate the certificate lifecycle on the device. If the certificate is absent on the device, Venafi automatically installs it. After that, each day, Venafi confirms the certificate version. As necessary, Venafi requests and installs an updated certificate on the device.
5. In the **Add a New Installation** window, find or create an existing device that requires certificate installation.
 - If the device already exists, search and select it. However, if the device already contains an installation of this certificate, a warning appears. Only add the device if you want multiple applications on a device to use the same certificate.
 - If the device is missing, click **Create a New Device**, and then provide the device address and the folder location where the device should be stored.
6. On the same window, specify any other information as required. For example:
 - If tracking requires validation, specify a port number.
 - If necessary, select a driver as the **Installation Type**.
7. Click **Add Installation** or if you want the device to have more than one copy of the certificate, click **Add Anyway**.

8. *If you are automating the installation of the certificate on this device, "Edit a certificate's installation details" on page 483.*
9. *If you are manually installing the certificate on this device, click **Download Certificate**. If necessary, specify certificate format, chain order, and password, and then click **Download Installation**.*

IMPORTANT When the Add Installation wizard completes, you still need to take the certificate you've downloaded and install it on the target device. Failure to do so will result in inaccurate reporting in Trust Protection Platform.

About deleting installations

If you need to disassociate a certificate from a device, you can delete the installation. In this manual process, you locate the installation you don't want to track in Trust Protection Platform, and delete it. Deleting an installation *does not* delete any certificates or keys on devices.

IMPORTANT If the certificate is still on the device and is not retired, and the device is scanned by discovery, the installation will be re-created.

When viewing a certificate in Aperture, click **Installations** in the side bar to see the installations associated with a certificate. Each installation row has an action button with the option to delete the installation. You must have the `delete` permission on the device to see the delete option in the action button.

IMPORTANT If you are working with Apache installations that remotely generated keys and a CSR using an HSM and there are less than two remaining installations after the deletion, Aperture automatically removes the Application group. For more information, see "[Delete a certificate installation](#)" below.

Delete a certificate installation

When you delete a certificate installation, you remove the Application object that controls provisioning for a certificate. If you are working with Apache and there are less than two remaining installations that generated from a remote CSR generation, TLS Protect automatically removes the Application group in Policy Tree.

IMPORTANT If you are working with Apache installations that remotely generated keys and a CSR using an HSM and there are less than two remaining installations after the deletion, Aperture automatically removes the Application group. For important information about deleting installations, see "[About deleting installations](#)" above.

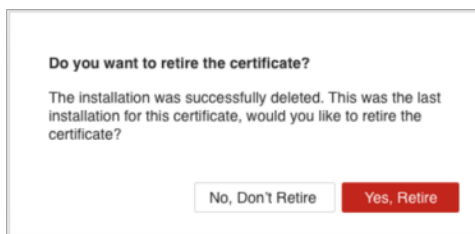
TLS Protect automatically removes the group for the following reasons, when you:

- Delete the certificate.
- Delete all installations for the same certificate.
- Move all installations to a different certificate.

IMPORTANT You must have the *View*, *Read*, and *Delete* permissions in order to complete this task.

To delete a certificate installation

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Open the certificate that has the installation you want to delete.
3. Either expand the installations by clicking the **down arrow** next to the number of installations, or open the certificate details page and click **Installations** in the side bar.
4. Locate the installation you want to delete, click the down arrow on the action button, and then click **Delete**.
5. In the pop up window, confirm you want to delete the installation by clicking the **Yes, Delete** button.
6. If the installation that you delete is a certificate's last installation, you will see an option to retire the certificate after the installation is deleted. To retire, the certificate, click **Yes, Retire**. Otherwise, click **No, Don't Retire**. For information on certificate retirement, see ["Retiring a certificate"](#) on page 465.



Creating a new user credential for certificate installations

When automatically installing certificates onto devices, there are two technology options: agent or agentless. The agent method uses the [Venafi Server Agent](#)¹ while the agentless method relies on the Venafi Trust Protection Platform either having the credentials to authenticate to the system, or access to the credentials on a password management system, like [CyberArk](#)²

Create a new user credential (Certificate Details)

1. From the [TLS Protect](#) menu bar, click **Inventory**, and then click **Certificates**.
2. Open a certificate details page by clicking on a certificate name, and then click **Installations**.
3. Click the **Edit** quick action for one of the installations.

There are several places in the Installation Settings window that request credentials.

4. For any credential field click **Create New Credential**.

The following image shows an example of the Installation Settings window for an Amazon installation. The fields displayed vary depending on the installation type.

The screenshot shows the 'Installation Settings' window. It has a black header with the title 'Installation Settings'. Below the header, there's a 'Created On' field with the value '1/24/2017 7:13 AM'. The main content is divided into two sections: 'Device' and 'Connection Information'. The 'Device' section has three fields: 'Device Folder' (with the value 'Policy/Devices'), 'Hostname/Address' (with the value 'localhost'), and 'Device Credential' (a dropdown menu with 'Choose Existing Object' and a 'Create New Credential' link). The 'Connection Information' section has three fields: 'Access Key ID' (a dropdown menu with 'Choose Existing Object' and a 'Create New Credential' link), 'Secret Access Key' (a dropdown menu with 'Choose Existing Object' and a 'Create New Credential' link), and 'Secret Access Key' (a dropdown menu with 'Choose Existing Object' and a 'Create New Credential' link'). At the bottom right, there are 'Cancel' and 'Save' buttons. Three red arrows point to the 'Create New Credential' links for the Device Credential, Access Key ID, and Secret Access Key fields.

5. Update the credential fields.

¹For more information on working with Server Agents, refer to the Server Agent Installation and Configuration Guide.

²You can read more about CyberArk's Enterprise Password Vault in the Trust Protection Platform Administration Guide.

The following table lists fields that may appear on the form, depending on the type of credential needed:

Field	Description
Folder	Select the folder where the credential will be stored.
	TIP Some clients like to store all credentials in a single folder; others prefer to keep the credentials stored relative to the certificates or devices that use the credentials.
Credential Name	This is the display name of the credential that you will see in Trust Protection Platform when you are viewing the list of credentials.
User Name	Enter the user name to connect to the device.
Password	Enter the password to connect to the device.
Confirm Password	Re-enter the password to confirm you have entered it correctly.

6. Click **Save**.

Edit the Installation Type

Often times when installations are created through discovery, you aren't able to detect the type of appliance, software, or keystore the certificate is being used on, so by default a "Basic" installation is created. As you learn about your inventory, you can update the installation type to something more accurate that also adds support for automatic installation of the certificate.

IMPORTANT You must have the *Write*, *Create*, and *Delete* permissions in order to complete this task.

Edit the installation type for basic installations

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. If you know the certificate that has the Basic installation you want to change, locate it and open it.

You can use the **Installation Type** filter in the **Common Filters** filter group to help you find Basic installation types.

3. Locate the certificate with the installation you want to edit.

4. Either expand the installations by clicking the **down arrow** next to the number of installations, or open the certificate details page and click **Installations** in the side bar.
5. Locate the installation that is Basic, and in the action button click **Set Installation Type**.
6. From the **Installation Type** drop-down, click the new installation type, and then click **Save**.

NOTE If the type is not *Basic*, you can't change an installation type unless you delete the installation and create it again.

Edit a certificate's installation details

IMPORTANT You must have the *View* and *Write* permissions in order to complete this task.

To edit a certificate's installation details

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Locate the certificate with the installation you want to change.
3. Either expand the installations by clicking the **down arrow** next to the number of installations, or open the certificate details page and click **Installations** in the side bar.
4. Locate the installation you want to edit, and then click the **Edit** action button.
5. Make the desired edits.

The available fields depend on the Installation type. If you are enabling remote key generation follow the appropriate instructions:

- Apache: [Enabling remote key generation for Apache certificates](#).
 - CAPI: [Enabling remote key generation for CAPI certificates](#).
 - JKS: [Enabling remote key generation for JKS certificates](#).
6. To save your changes, choose one of the following options (if multiple options are available):
 - **Save Installation Settings**. This option will save the changes, but won't attempt to actually install the certificate on the device. This option is always available.
 - **Save and Install**. This option will save the changes, and will begin the process of provisioning the certificate to the device. This option is only available when the certificate is configured for installation, and has never been installed before.

TIP For information on adding new credentials while editing the installation settings, see "Creating a new user credential for certificate installations" on page 481.

Approve or reject a workflow ticket for a certificate installation

As an approver for a workflow ticket, you need to take action to either approve or reject a proposed certificate installation.

NOTE You must be the assigned approver for a workflow ticket assigned to the installation to see the **Approve/Reject** action.

Take a workflow action on a certificate installation

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. In the Quick Filters section, click **Pending My Approval**.
3. Locate the certificate that needs approval.
4. Click **Approve/Reject**.
5. Review the information in the confirmation modal, then either click **Approve** or **Reject**.

Cancel a certificate installation

Canceling and attempted installation stops the processing for the installation and clears the errors, resetting the installation so you can remedy the issue and attempt to reinstall the installation, if desired.

Canceling will stop all certificate processing, but will not delete any certificate data.

NOTE You must have *write* permissions to the installation, and the installation needs to have encountered an error during the installation attempt to see the **Cancel Request** action.

To cancel a certificate installation

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. In the Quick Filters section, click **In Error**.
3. Locate the certificate for which processing should be canceled, and then click the down arrow on the action button, and then click **Cancel Request**.

4. Review the information in the modal window about canceling a request.
5. When your review is satisfactory, click **Yes, Cancel Renewal**.

Retry a certificate installation

When an attempted installation resulted in an error state, you can retry the last attempted step in the installation process.

NOTE The **Retry Renewal** action will only be available if the installation encountered an error during the installation attempt, and if you have the *write* permission to the installation.

To retry a certificate installation

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. In the Quick Filters section, click **In Error**.
3. Locate the certificate that needs to be retried, click the down arrow on the action button (if necessary), and then click **Retry Renewal**.

Replace a certificate installation

You may find that you need to replace a certificate on a device with a different certificate, essentially changing the certificate associated with the installation.

NOTE You must have *view* and *write* permissions to the installation to replace a certificate. You must also have *view* and *write* OR *view* and *associate* permissions to the new certificate that you want to replace with.

To replace a certificate installation

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. Using the Filters, locate the old certificate that you want to replace, and then click the certificate name to open the certificate details.
3. Click **Installations** in the side bar.
4. Locate the device the certificate is currently installed on, then in the quick action button, click the down arrow, and then click **Replace**.
5. In the Replace Certificate dialog box, search for the new certificate to associate with this device.

6. Click the **Replace** button.
7. Click **Install**.

IMPORTANT If you don't Install, the certificate will be replaced only in inventory but will not be replaced on the device.

When the certificate details window refreshes, you'll see the new certificate, and you can see new the device installation.

About adding an installation to a certificate

You can easily create an installation for a certificate on a specific device. The action is called **Add Installation**.

The **Add Installation** action is not available if any of the following are true:

- The certificate state is *Lost*, *In Error*, or *Retired*
- The certificate is renewing, or has not yet been issued
- The certificate management type is *Unassigned*

For more information on adding an installation, see ["Creating a certificate installation" on page 476](#).

Running validation scans

By default, validation scans occur daily according to the daily task schedule configured on the Trust Protection Platform server object in the Platforms tree. However, you can also manually run a validation scan.

Trust Protection Platform runs a validation whenever a certificate is automatically renewed and installed. This is called *SSL/TLS validation*.

To run a manual validation scan

1. From the Aperture menu bar, click **Inventory > Certificates**.
2. Find the certificate that you want to validate.
3. Click the certificate's nickname.

4. On the certificate's details page, click **Actions > Validate Now**.

When you click **Validate Now**, it triggers validation of the certificate and all of its installations.

The Validation statuses change to *In Process*.

The page automatically refreshes when the validation is complete.

5. To see more detailed validation results, switch to the **SSL/TLS** tab on the left.

To see what each validation result means, see ["Review validation results" on page 548](#).

Frequently Asked Questions

Q. Can there be more than one Aperture Configuration Object? Can I move it around?

You can have only one Aperture Configuration Object at a time but you can move it around anywhere in your Policy tree.

Q. Can a person transfer his or her access or profile to someone else when they go on vacation?

No. For security reasons, transfers of access are not allowed. However, if two people need access to the same folders and certificates, consider putting them in the same Group and give the Group the correct permissions.

Q. Can two or more users access the same certificate at the same time?

Multiple users can read a certificate at the same time. If multiple users attempt to write a certificate at the same time, only the changes made by the last user will be saved.

Q. What if my certificate creation or renewal process gets stuck?

The process may need to be restarted or reset and can be done only in Trust Protection Platform. Contact your Trust Protection Platform Administrator for help.

Q. What is the difference between monitoring and enrollment?

Monitoring

Organizations can monitor keys and certificates. TLS Protect helps monitor existing certificates and provides current information about the certificate. When the certificate is about to expire, messages are automatically sent to certificate owners, consumers, and approvers.

Monitoring **does not renew** the certificate. The administrator has to manually create the CSR (Certificate Signing Request), send it to the CA (Certificate Authority), then retrieve and install the renewed certificate.

Enrollment

Enrollment allows TLS Protect to **automatically renew** certificates. TLS Protect can generate and submit CSRs to Certificate Authorities using the parameters defined in the corresponding CA Template objects. Or, administrators can manually generate the CSR, then upload it to TLS Protect to complete the enrollment process.

After the CA signs the certificate TLS Protect retrieves the certificate. The administrator can then download the certificate and install it as needed.

Q. What does this message mean? *The user has additional certificates but your permissions do not allow you to see them. In order to view all certificates, the correct permissions need to be set.*

You'll see this message after you do a user name search for certificates. If you have fewer permissions than the user whose certificates you are trying to view, you'll be notified that there are more certificates. Extended permissions are needed in order to see them. Contact your Administrator for help.

Q. Why don't I see the Certificates menu?

The Certificates menu is only shown if your user account has read or view access to at least one certificate. If you create a new certificate, the Certificates menu will be shown immediately. If somebody grants you access to a certificate, you will see the Certificates menu the next time your log in.

Q. Why do I get a "403 Forbidden" error message when I'm logged in to the system?

Trust Protection Platform has security settings that protect the system from various types of vulnerabilities. If the system detects that the referrer header is not from an authorized source, you will see a "403 Forbidden" error message.

This setting is controlled by the registry of the Venafi Platform server. If you have a need to disable this security feature (not recommended), you can add the following registry key on all Venafi Platform servers that are in the cluster:

Registry Key location	Key Name	Data Type	Key Value
HKEY_LOCAL_MACHINE\Software\Venafi\Platform	DisableSameOriginCheck	Dword	1

How certificate renewal works

Whether you are having certificates renewed automatically or manually, it is important to understand how certificate renewal works.

When a certificate record is created in Trust Protection Platform, there are a couple of settings that affect the renewal behavior of the certificate. These settings can either be set by a policy that is applied to a certificate, or at the certificate level itself. These settings are:

- **Disable automatic renewal:** By default, automatic renewal is enabled for certificates in Trust Protection Platform. If you want to disable automatic renewal, you can set this value to *Yes*.
- **Renewal window:** This is the number of days before expiration that you plan to renew certificates. Many organizations pick a value between 30 and 90 days, to ensure there is time for all the necessary approvals and processes to ensure the renewed certificate is properly in place before the old certificate expires.

Remember that a certificate is an object with a finite lifespan. The process for how a certificate is renewed varies by CA, so check your CA's documentation on how this process works. Generally speaking, renewals don't just extend the validity date of the existing certificate. When you *renew* a certificate, you are actually getting a new certificate that has the same data as your old certificate, however the renewed certificate is a distinct object that needs to be downloaded and installed.

When you request a certificate, there is a transaction ID that is like an order number with the CA. Trust Protection Platform stores this transaction ID as a hidden field for the current version of the certificate. When you request a renewal, if your CA uses the Transaction ID field, the transaction ID is passed to the CA. This tells the CA that you are renewing a certificate that was issued by that CA previously.

This is important because many CAs use the transaction ID to extend the validity of a renewing certificate to ensure no time is lost when you renew a certificate early. The CA doesn't want you to wait until the last minute to renew your certificate, so many CAs will extend the expiration date to match the valid term of the prior certificate.

EXAMPLE Suppose that you acquire a certificate in January 2022, and your certificate is valid for 12 months. The expiration date of the certificate will be January 2023. Let's say that in Trust Protection Platform the renewal window is set to 90 days. In October 2022, Trust Protection Platform is going to tell you it is time to renew your certificate. You create a CSR to reissue the certificate for another 12 months.

Two things can then occur:

- If the CSR *does not* include the transaction ID of the original certificate, the CA doesn't see this request as being a renewal, and it will treat it as a new request. Since this is a new request being submitted in October 2022, the expiration date will be October 2022. In this case, you will lose three months of value of the original certificate.
- If the CSR *does* include the transaction ID of the certificate, the CA will recognize the request as a renewal, and will take into consideration the expiration date of the original certificate. The renewed certificate, even though it was submitted in October 2022 will be set to expire in January 2023.

Implications for renewing reverted certificates

Trust Protection Platform allows you to see historical versions of a certificate, so you can track or revert to a historical version. However, Trust Protection Platform only stores the transaction ID for the most recent certificate, not for historical certificates, so when you revert to a previous certificate, the transaction ID information is cleared. This means that if you revert to a historical version of a certificate, and then try to renew the certificate, there will be no transaction ID, and the CA will treat it as a new request. This means that if you may lose time on your certificates if you renew early.

Sorting certificates in the Policy Tree Certificates grid

Here is a list of columns that **cannot** be sorted in Policy Tree certificate grid.

NOTE If the column isn't listed here, it can be sorted.

Columns that cannot be sorted

Approver(s)

Contact(s)

Enhanced Key Usage

Key Usage

Organizational Unit

SANs (all)

Templates

About Domain Components

The Domain Components feature is an advanced feature in Trust Protection Platform that allows domain components to appear in certificates. This could allow you, for example, to use client authentication certificates to restrict the access of the certificate to the sub-domain specified on the certificate using the domain component attribute. This setting should only be used if the application server you are authenticating to is configured to support verification of domain components.

If your application servers are configured to support verification of domain components, Trust Protection Platform allows you to enable the domain components feature, which does the following:

- Shows you the domain components
- Allows you to specify, via policy, allowed domain components
- Allows you to specify on a certificate signing request the allowed domain components (if enabled by policy)

NOTE This is not a commonly used feature in Trust Protection Platform. If you have any doubt about whether you should enable this feature, leave it disabled.

If you leave this feature disabled, and a user attempts to upload a CSR with specified domain components, the CSR will be rejected by Trust Protection Platform. Users will need to re-create the CSR without domain components specified and upload the new CSR to continue.

If this feature is disabled, it also means the domain components field will be hidden on the new certificates form when Trust Protection Platform is generating the CSR.

Controlling domain components by policy

If your organization uses domain components to limit sub-domains on a certificate, you can enable this setting in the policy settings.

NOTE This is not a commonly used feature in Trust Protection Platform. If you have any doubt about whether you should enable this feature, leave it disabled.

To enable the domain components feature

1. From the **TLS Protect menu bar**, click **Configuration > Folders**.
2. Click the folder where you want to apply this policy setting.
3. Click the **Certificate Policy** tab.
4. In the **Subject DN** section, select **Allow Domain Component**.
5. If desired, lock the value using the lock icon.
6. If you want to restrict all certificates created in this folder to a specific domain component setting, specify the **Domain Component**.
7. If desired, lock the value using the lock icon.
8. Click **Save**.

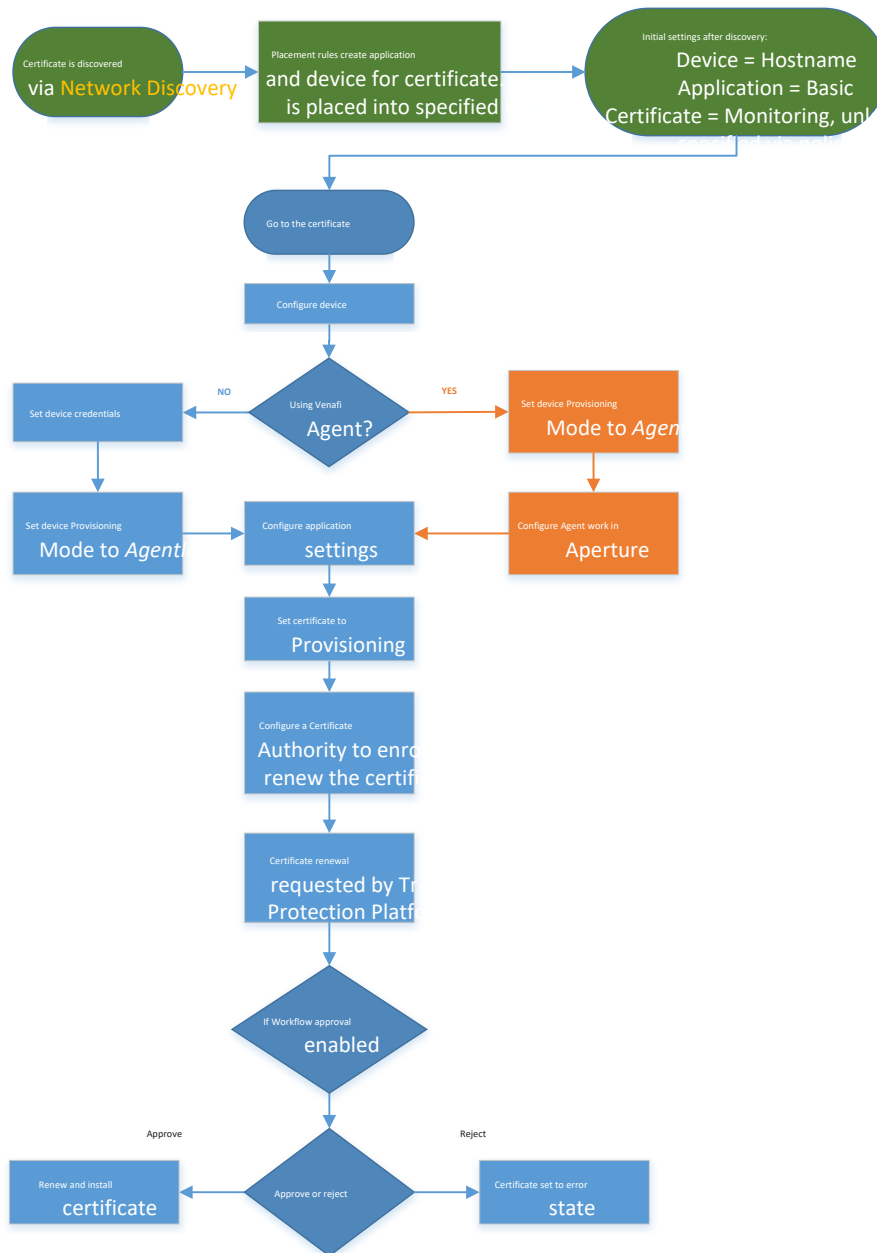
The new settings will be applied to this folder, and all sub-folders in the tree.

12

Certificate installation

Certificate installation (Provisioning) provides fully automated certificate lifecycle management—it automatically requests, installs, renews, and monitors your system's certificates, producing consistent and repeatable processes that improve security as well as reduce operational and compliance risks.

The links below the chart mirror the steps in the flow chart. As you follow the steps in the diagram, click the corresponding link to learn how to complete the task.



For information on how to decide whether to use agent or agentless certificate installation, see ["About certificate installation methods: agentless versus agent"](#) on page 496.

For an explanation of the managed stages of the certificate lifecycle, see ["About certificate lifecycle management"](#) on page 27.

This chapter contains the following topics:

About certificate installation methods: agentless versus agent.....	496
Configuring devices for certificate installation.....	498
Managing applications.....	509
Changing the management type to Provisioning.....	511
Configure a Certificate Authority to enroll and renew the certificate.....	512
About workflow objects used during certificate installation.....	512
Installing (provisioning) lots of certificates and keys at one time.....	514
Renewing a certificate manually.....	529
Installation statuses explained.....	531
Validating a certificate's installation (onboard validation).....	533

About certificate installation methods: agentless versus agent

Trust Protection Platform can install certificates on devices in your network with or without using the Server Agent. If for some reason Trust Protection Platform can't connect to the device on which you plan to install the certificate (firewall restriction or no existing route to the subnet, for example), you have an alternate connection method.

Learn about [Supported shells](#) used to establish a connection between Trust Protection Platform and a client.

Method	Description	Use if...
Agentless	Installs certificates to devices in your network using credential authentication between Trust Protection Platform and other network devices. <i>Advantages:</i> Typically the easiest method to use—when you have large numbers of devices that are configured similarly—because you do not need to install or maintain any additional software on the devices where you plan to install certificates (unless remote generation is required, in which case the applicable crypto utilities must be installed). Also, Trust Protection Platform automatically creates the necessary device and credential objects during Discovery. <i>Requirements :</i> You must set up and manage device credentials for every device where you want to install certificates.	■ You have many devices that have similar configurations (use the same management credentials, use standard keystore locations, etc.) ■ Keystores are installed to the same location (path) on all of your devices ■ You do not want to perform routine scanning of trust assets on your devices

Server Agent

Install certificates to devices in your network using Server Agents that are installed on those devices (Server Agent-enabled devices).

See [Server Agent-supported keystores](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Advantages : A powerful method that can reduce the amount of work required to configure and manage trust between Trust Protection Platform and the agent-enabled devices where you plan to deploy certificates. Especially true if you do not use similar configurations across devices where you want to install certificates. As certificates are discovered, Trust Protection Platform creates the necessary objects so that it can manage the discovered certificates almost immediately.

The agent method also helps with load distribution because installed Server Agents use the system resources on the devices where they are installed; in the case of Agentless, all of the work performed is on the Trust Protection Platform server. With agent, rather than one device performing hundreds of tasks, you have hundreds of devices performing a few tasks each.

Requirements : Configure and deploy the Server Agent to each device on which you plan to install (and manage) certificates.

- You have many devices that have *dissimilar* configurations (use many different management credentials, keystore locations vary from server to server, etc.).
- Keystores need to be installed to different locations on a per server basis (the Discovery process identifies where the keystores are and then automatically creates the required objects).
- You want to perform routine scanning of trust assets on all of your devices

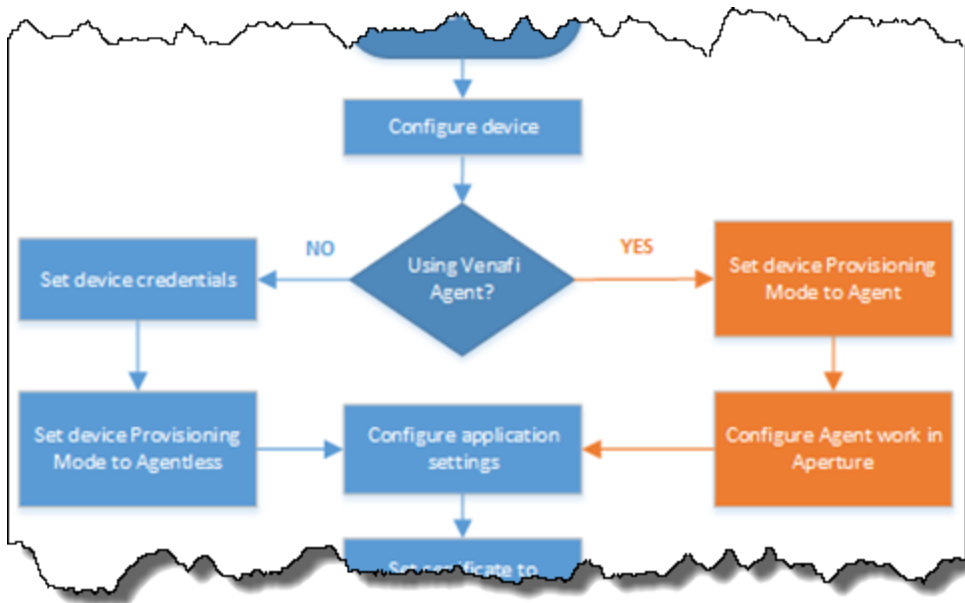
EXAMPLE Which method you choose depends on which platform (OS) will be hosting the certificate and which keystore formats are required. Consider the following scenarios:

- *Agentless or Agent methods*: If you have a Unix or Linux system and you need JKS, PEM, CAPI, or PKCS#12, you could use either agent or agentless, depending on which method best fits your organization.
- *Agentless method only*: If you have a network appliance like F5 Big-IP LTM, Citrix NetScaler, vThunder, IBM DataPower, etc., then the Agentless method is your only option because these are closed systems where the agent is not supported.
- *Agent method only*: If you have a Windows system and you need CMS (GSK), JKS, PEM, CAPI, or PKCS#12, then the agent is the more realistic choice. This is because Venafi requires a third-party SSH server to be installed on Windows in order to support them using the Agentless method.
- *Agentless or Agent methods (Conditional)*: Network restrictions (and associated architecture) can determine which method you use. For example, if Trust Protection Platform can connect to the device on which you plan to install a certificate but the device cannot contact Trust Protection Platform, then your only option is to use Agentless; this is because during agentless certificate installation, Trust Protection Platform initiates the network connection. However, If Trust Protection Platform *cannot* connect to the device on which you plan to install the certificate but the device *can* contact Trust Protection Platform, then your only option is to use agent; this is because during an agent certificate installation, the device is the one that initiates the network connection.

Configuring devices for certificate installation

If you have chosen to install (provision) certificates without the Server Agent (Agentless), you need to set credentials on the device and set the device's Provisioning Mode to Agentless.

If you have chosen to use the Server Agent, then you need to make sure that the Provisioning Mode on the device is set to "agent."



- If you have chosen *Agentless*:

Configure device credentials and set the Provisioning Mode to Agentless. See "Setting, editing, or renaming devices and credentials (Agentless)" below and Device object settings (agent and agentless).

- If you have chosen *Agent*:

Set the device's Provisioning Mode to Agent. See Device object settings (agent and agentless).

Setting, editing, or renaming devices and credentials (Agentless)

Device credentials allow Trust Protection Platform to identify the correct device. The procedures that follow explain how to set device credentials and rename devices using the **Inventory > Devices** menu option in the SSL Protect console.

NOTE TLS Protect does not provide the **Inventory > Devices** menu option. However, you can use Product Switcher to switch to the SSH Protect console to see the menu option.

For more information about Product Switcher, see [Unified menu bar and SSO](#).

To set device credentials

NOTE You need the *View* and *Write* permissions in order to modify device credentials.

1. From the SSH Protect menu bar, click **Inventory > Devices**.
2. Using filters if needed, find the device you want to configure.
3. In the **Device** list, click the device you want to edit.
4. Click **Edit**.
5. In the **Edit Device Settings** area, add or edit the device's information.
6. When you're done, click **Save**.

To learn more, see [Device Object Settings](#).

To rename a Device

NOTE You need the **rename** permission to the device, or this functionality won't be available to you.

1. From the SSH Protect menu bar, click **Inventory** , and then click **Devices**.
2. Locate the device you want to change.
3. Click on the device name to open the details page.
4. Hover your mouse pointer over the device name until you see the name highlighted, and then click it.
5. In the **Rename** box, type the new name in the **New Name** field, and then click **OK**.

Object names may not contain the backslash \ or less-than sign < characters. Object names (including their path ancestors in the policy tree) must be fewer than 255 total characters.

Device object settings (agent and agentless)

To enable Trust Protection Platform to reference a device when it manages and validates certificates and private keys, you must configure the device object. This object provides the information Trust Protection Platform needs to reference a device.

To get to these settings on an existing object, open Policy Tree, locate the device in the Policy tree and then click the **Settings** tab.

BEST PRACTICE Consider managing device object settings via policy. For more information, see [Managing devices using policies](#).

IMPORTANT If you make any modifications to device object settings, you must click **Save** to implement those changes.

Field	Policy	Description
General		
Device Name	No	Unique name for the Device object. (Only visible when creating the device object.)
Description	No	Description of the device object.
BEST PRACTICE An effective description can be helpful to other administrators by describing the purpose or function of the device object.		
Contact		User or group Identities assigned to this object. Default system notifications are sent to the contact identities. The default contact is the master administrator.

To select the Device object contacts

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, then return the list of requested users or groups. If you want to display all user or group entries, enter the wildcard character (*).

2. Select a user or group identity, and then click **Select**.
3. Press **Shift+click** to select multiple, contiguous users and groups. Press **Ctrl+click** to select multiple, discontinuous users and groups.

Host Information

Hostname/Address No	IP address or hostname of the physical server associated with the device object.

Field	Policy	Description
		Trust Protection Platform supports both IPv4 or IPv6 connections.
		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.
Provisioning Mode		Specify whether provisioning to this device should be done using the Server Agent, or without the agent (called Agentless). If you are provisioning using the Server Agent, you must also then configure agent work in Aperture. For more information, see Creating and assigning Work. For Adaptable SSH Key Discovery, click Adaptable.
Concurrent Connection Limit		Maximum number of connections the server will accept from Trust Protection Platform. Currently, Trust Protection Platform uses only one connection to provision certificates and keys on a server. To configure this setting via Policy, go to the Devices > Device tab in the Policy object configuration. The Device Concurrent Connection Limit defined in the Policy object may be inherited by all subordinate Device objects.
Device Credential		Credential that Trust Protection Platform uses to authenticate with platforms or access keystores on the device.

Field	Policy	Description
		Credential objects store the credentials Trust Protection Platform uses to authenticate with devices, applications, and CAs. The stored credential may be a password, a username and password, a certificate, or a private key. Trust Protection Platform uses the Device Credential only if credentials are not defined in the application object. If multiple applications are running on a single device and they share the same credentials, you can simplify credential management by defining the required credential only on the device object. The device credential is then used for all subordinate applications and you don't have to define credentials for each application object. If you use the device credential to authenticate with your subordinate applications, the user account must have <i>read</i> and <i>write</i> permissions to the device object's Temp directory as well as the permissions required for each application. For more information on application permissions requirements, refer to the Permission Requirements sections for each application driver. To select the Device Credential 1. Click the Browse button. 2. In the Credential Selector dialog, select the Credential required to authenticate with this device, and then click Select. For more information, see Working with system credentials in the <i>Venafi Trust Protection Platform Administration Guide</i>. To configure this setting via Policy, go to the Devices > Device tab in the Policy object configuration, and use the Device Credentials setting. The Device Credentials defined in the Policy object may be inherited by all subordinate Device objects.

Temp Directory		Directory where Trust Protection Platform can write temporary files. ■ To configure this setting via Policy, go to the Devices > Device

Field	Policy	Description												
		tab in the Policy object configuration.												
		The Device Temp Directory defined in the policy object may be inherited by all subordinate Device objects.												
		For agentless discovery, the value of this field is used for .venafiTemp directories. (If a value is not in this field, agentless discovery will use the default directory of <code>/var/tmp/</code> .)												
OS Type		Specify the OS type of the devices you will connect to with this policy, or select Automatic .												
		TIP This field is not visible if the <i>Provisioning Mode</i> is set to Adaptable .												
Jump Server		(Optional) The jump server required to connect with the current device. A jump server is an intermediary server through which external servers, such as Trust Protection Platform, can access a device behind a firewall. For more information, see Managing Jump Server Objects. Trust Protection Platform supports jump server connections to the following supported applications using SSH: <table><tr><td>Apache</td><td>PEM</td></tr><tr><td>Cisco ACE</td><td>PKCS#12</td></tr><tr><td>GSK</td><td>Tealeaf PCA</td></tr><tr><td>iPlanet</td><td>VAM nShield</td></tr><tr><td>JKS</td><td></td></tr><tr><td>NetScaler</td><td></td></tr></table>	Apache	PEM	Cisco ACE	PKCS#12	GSK	Tealeaf PCA	iPlanet	VAM nShield	JKS		NetScaler	
Apache	PEM													
Cisco ACE	PKCS#12													
GSK	Tealeaf PCA													
iPlanet	VAM nShield													
JKS														
NetScaler														

To require a jump server connection for the current Device object

1. Click the **Browse** button.

Field	Policy	Description
		2. In the Device Selector dialog, select the device object required to connect to this device, and then click Select. When you create a Device object under a Device object, Trust Protection Platform automatically assigns the parent Device object to the Device. However, this is not required, You can associate a Device object with any Device object in the Policy tree.
Use Sudo		Select Yes to enable sudo. If you need to be able to provision certificates to secure locations for which the user account you're using does not have access rights, sudo can be used to temporarily elevate the user rights in order to perform provisioning tasks on a Unix server. When enabled, Trust Protection Platform provisions to a temporary directory where your user account has permissions to perform basic functions; then sudo is used to copy the files from the temporary directory to the target directory where they need to be placed. For more information about sudo, see About using sudo. NOTE Sudo use only applies to SSL CLI-drivers that use a standard shell and CLI-based drivers (Apache, JKS, GSK, iPlanet, PKCS#12, and PEM).
Sudo Credential (Optional)		Select the credential to use with sudo, which in this case is simply a password. This is the password that sudo asks for by default when a user attempts to run a command using sudo. The password is optional because the device administrator can put NOPASSWD in the sudoer's file, thereby allowing the user to execute the command without being challenged for a password. For more information about sudo, see About using sudo.
Enforce Host Key		Describes how to handle SSH connectivity when the Provisioning Mode is <i>Agentless</i>. Matches the presented key and corresponding thumbprint with information in Trust Protection Platform.

Field	Policy	Description
		Set the Enforce Host Key to <i>No</i> (default), if you want host connectivity regardless of thumbprint changes. Trust Protection Platform compares the current device thumbprint with the last seen fingerprint. If the fingerprints differ, log event is <i>40060020, SSH Public Key Fingerprint Changed</i>. Set Enforce Host Key is <i>Yes</i>, if you want to block host connectivity after the thumbprint changes. If the presented thumbprint is different than the stored thumbprint, Trust Protection Platform. refuses the connection. The log event is <i>40060004, SSH Connect To Host Failed</i>. For example: <i>127.0.0.1, 2/22/2017 10:10:04 AM, \VED\Policy\centos-oracle: \VED\Policy\centos-oracle, Error: Error, Translated event: SSH Connection Failed, The SSH library failed to connect to 192.168.3.220 on port 22, with the Connection Result 8: The host key was not accepted.</i>
Presented Thumbprint	n/a	For devices that use the Agentless mode to provision. When the Enforce Host Key is <i>Yes</i> , this field shows the SSH server key thumbprint, also known as a fingerprint, that Trust Protection Platform detected after a successful connection to the device.
Presented Key Type	n/a	The key type that encrypted the thumbprint. Corresponds to the Presented Thumbprint value.

TIP The remaining settings in this list **ONLY** apply (and are thus only visible) if you set the *Provisioning Mode* to **Adaptable**.

Adaptable Script Parameters

PowerShell Script		The PowerShell script you want used for this policy. The script must be stored in the <code>\Venafi\Scripts\AdaptableSSHManagement</code> folder on the Venafi server. For more information about PowerShell scripts for Adaptable SSH Key Discovery, see PowerShell script reference for Adaptable SSH Key Discovery.

WebSDK OAuth Token Configuration

Adaptable SSH Key Discovery can use Venafi APIs for communicating between devices. An API integration needs to be created for this purpose. To learn more about working with and configuring API integrations, see [About API integrations](#).

Field	Policy	Description
OAuth Application Id		The value of the Client ID of the application from the API Integrations inventory.
OAuth Token Credential		The username credential object that contains the username and password of the identity that has access to the specified application. (This can be any SSH Protect identity that can obtain a grant for this application.) When looking at the application in the API Integrations inventory, click on an application name, and look at the User or Team access section to see which users can obtain grants
OAuth Scope		This scope must exactly match the scope, privileges, and restrictions for this application as they are displayed in the API Integrations inventory. The easiest way to copy this is to open the application details from the API Integrations inventory, and in the Overview section, copy the value of the scope attribute in the JSON example. At <i>minimum</i>, the application must have the following: Scope Privileges and restrictions ssh discover If your application uses this minimum setting, you would enter this value: <code>ssh:discover</code> If you want to do SSH remediation on the devices, you will need the following minimum scope: Scope Privileges and restrictions ssh manage,discover If your application uses this setting, you would enter this value: <code>ssh:manage,discover</code>

Advanced Settings

Field	Policy	Description
Enable Debug Logging		If you are trying to troubleshoot a problem with your Adaptable SSH Key Discovery setup, you may consider enabling this setting to get debugging information in the logs.
Script Execution Timeout		The maximum number of seconds a script can run before the process is terminated.
Custom Fields		
If you have configured custom fields, you can set the field value on for the policy here. You will have a separate field for each custom field you have created. For more information, see Adding or deleting a custom field .		
These custom fields are NOT passed to the PowerShell script, and are not related to the adaptable technology features of Venafi Platform.		

What's next?

After you create a CA object, you can select it from the Policy tree, and then view important information and manage various settings.

- Click the **General** tab to view and modify log and permissions settings.
 - Click the **Log** sub-tab to view any logged events that are triggered by the template object.

IMPORTANT You must have the *Read* permission to view the Log tab.

For more information about options found on the Log tab, see [Viewing log events](#).

- On the **Permissions** sub-tab, you can configure the users or groups to whom you want to grant permissions to the new template object.

Consider managing object permissions via parent objects so that you can take advantage of inheritance. For more information, see [Permission inheritance and flow down](#).

Using the Server Agent to install certificates

If you are going to install certificates to devices using the Server Agent, you need to configure Certificate Installation work that can be pushed out from Trust Protection Platform to agent-enabled devices.

For more information about setting up Certificate Installation work for installed agents and their devices, see [Setting up certificate installation work](#) in the *Server Agent Installation and Configuration Guide*.

Managing applications

Application objects represent the server platforms or keystores where Venafi Trust Protection Platform™ manages certificates and private keys. Depending on the level of certificate management configured on the certificate—monitoring, enrollment, or provisioning—Trust Protection Platform can request, enroll, renew, install, and validate the certificate on the application object's associated platform or keystore.

NOTE For more information about monitoring, enrollment, or provisioning, see ["About certificate lifecycle management"](#) on page 27.

Trust Protection Platform can also perform certificate and key management functions on managed applications, including generating, extracting, or pushing the private key associated with a managed certificate to the application object's associated platform or keystore.

For more information about configuring application objects for use with supported Venafi application drivers, see [Managing applications](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Editing an application

During Network Discovery and Agent Discovery, *devices are created when certificates are discovered*. Placement rules allow this to happen automatically. You might want to change the application on a device or edit its settings.

Management Partitions allow you to specify which processing engines are allowed to perform validation scans. Partitions allow you to work around firewalls and network routing issue. To learn more, see [Using Management Partitions](#).

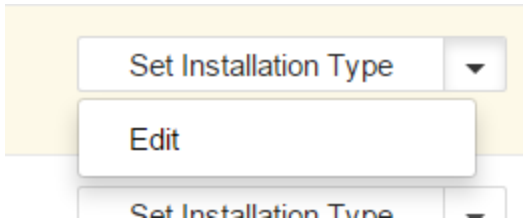
To change the application settings on a device

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Find the certificate that is associated with the application.
3. Click the certificate's name.
4. In the sidebar, click **Installations**.
5. To set the installation type, click **Set Installation Type**.

Setting the Installation Type is required before you can provision the certificate.

Once you set the Installation Type it cannot be changed. If you need to change the installation type after it has been set, you will need to add a new installation using the Web Admin console.

6. To edit the installation information, click **Edit**, or click the **Set Installation Type** arrow, and then click **Edit**.



7. When you click the **Edit** option, the **Installation Settings** window appears.
8. In the **Installation Settings** window, edit the application settings as needed.

The Installation Settings window is grouped into sections; the sections and options shown will depend on the installation type and other settings.

A screenshot of the 'Installation Settings' window. The window has a black header with the title 'Installation Settings'. Below the header, there is a 'General' section. The 'General' section contains several fields: 'Name*' with the value 'App-443', 'Type' with the value 'Basic', 'Description' (empty), 'Processing Enabled' with radio buttons for 'Yes' and 'No' (selected), 'Contact(s)' with the value 'local:Admin', 'Approver(s)' with the value 'local:Admin', and 'Created On' with the value '3/5/2015 7:38 PM'. Below the 'General' section, there is a 'Device' section which is currently empty. At the bottom right of the window, there are two buttons: 'Save' and 'Cancel'.

9. When you're done, click **Save**.

Changing the management type to Provisioning

You can change the Management Type of a certificate in two different ways. If the certificate's settings are locked at the policy level, then you must edit the policy.

IMPORTANT You must have the **View** and **Write** permissions in order to make changes.

To edit an individual certificate's management type

1. To learn about management types, see ["Functional overview"](#) on page 22.
2. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
3. Using **Filters** or **Search**, find the certificate you want to edit.
4. Click the certificate's name.
5. In the certificate's details window, click **Renewal Details**.
6. Click **Edit**.
7. (Conditional) If the management type isn't locked at the policy level, then you can change the **Management Type**.
8. When you're done, click **Next**.
9. Click **Close**.

To edit a management type at the policy level

1. From the **TLS Protect menu bar**, click **Configuration > Folders**.
2. From the list, click the folder (policy) you want to edit.
3. In the sidebar, click **Certificate Policy**.
4. Under **General Settings**, change the **Management Type**.
5. Click **Save**.

To learn about certificate object settings, see ["About certificate object settings"](#) on page 146.

Configure a Certificate Authority to enroll and renew the certificate

The CA Template object defines the information Trust Protection Platform needs to connect to a certificate authority (CA) so that it can submit a certificate signing request (CSR) and retrieve certificates from the CA during enrollment and installation operations.

To learn more about how CA Templates work and how to configure them, see [Certificate Authority Overview](#).

About workflow objects used during certificate installation

Workflow objects define the parameters for certificate approval. They can also inject a local command at a specified stage of the certificate lifecycle.

NOTE You must have the **Create** permission to the policy in which you want to create the workflow object.

To learn more about workflow objects, see "[Creating a certificate workflow](#)" on page 560.

Approving or rejecting a certificate installation

When you set up a workflow that requires an approval and assign it to a policy, in Aperture you can approve or reject the certificate renewal.

IMPORTANT For certificate installation, approvals can be scheduled **ONLY** for stage 800.

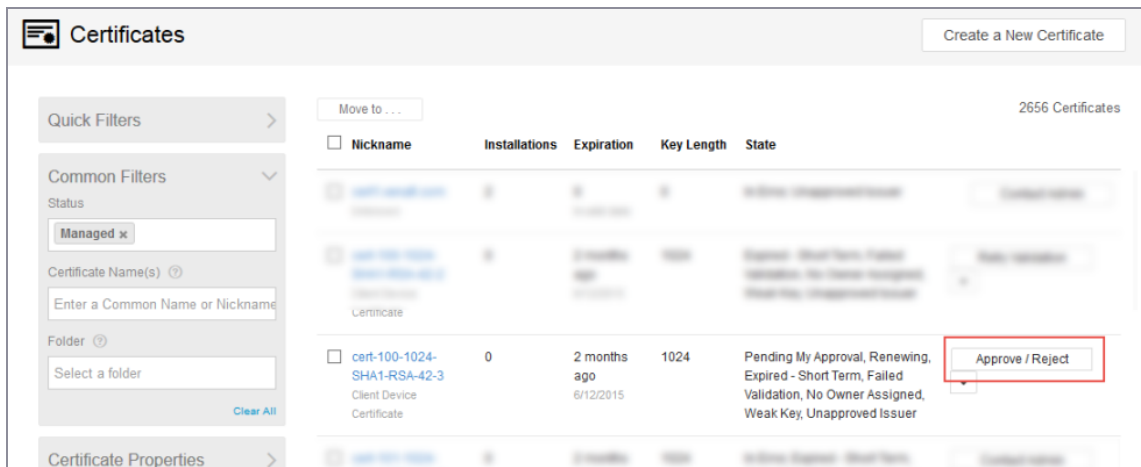
You can take action on a certificate either from the certificates list, or from the certificate details screen.

To approve a certificate installation in Aperture

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Find the certificate that you want to approve.

You can use filters to help you narrow the search results.

3. In the certificate list, click **Approve/Reject**, or in the certificate detail page, click **Approve/Reject**



4. Review the details about the certificate installation, and then click **Approve** or **Reject**.

On the certificate list, the state changes to **Renewing**.

Configuring certificate workflow approval to receive notifications

Venafi Trust Protection Platform™ allows for certificate installation (provisioning) workflows to be approved in TLS Protect. If you have previously customized SMTP Channels for workflow notifications, you will need to update them so the link directs users to the correct location in the modern interface.

Customers using the default templates for workflow notifications do not need to take any action.

Part 1: Determine if you're using default or customized SMTP notifications

1. Log into the Venafi Configuration Console (VCC) or install the Tools MMC snap-in and open it).
2. In the **Tools** node, expand **Logging > Notification Rules**.
3. Expand **Built-in > Certificate**.
4. Locate the rule **Workflow Approval Pending**.

If the **From Factory** column is set to **Yes**, the default notification is being used and no changes are required.

If the **Disabled** column is set to **Yes**, and you have a notification rule triggering on workflow, then you have custom notifications, and you need to continue to Part 2, below.

Part 2: Update the SMTP macro

1. Log into VCC (or install the Tools MMC snap-in and open it).

If your Notification Rule was **Disabled** in Part 1, above, and you have a notification rule triggering when a workflow is pending, then you need to look in **Tools > Logging > Notification Rules** for a custom rule that is triggered on the **Workflow Ticket Issued** event. Make note of the Target SMTP channel that rule is pointing to.

2. Navigate to your custom SMTP rule that notifies your users when there is an workflow requiring their approval.
3. For details on creating or editing notification rules, see "[Creating notification rules](#)" on page 432.
4. When making changes to logging channels, it is a good idea to restart your Venafi Log Server service to make sure the changes take effect immediately.

Installing (provisioning) lots of certificates and keys at one time

If you need to provision a large number of certificates and keys to multiple devices, you can create a *Bulk Provisioning* job in Aperture and either run it manually, or according to a defined schedule.

When you configure your Bulk Provisioning job, you specify one or more source folders where you'll place your certificates and keys to be provisioned. When the job is run, it checks the folder and provisions certificates and keys found there to one or more devices and folders you specified in the job settings.

Bulk Provisioning jobs that have run successfully are triggered automatically when new certificates appear in the source folders you've specified in the jobs settings. This is also true when existing certificates are imported with their private keys.

Bulk Provisioning is designed to minimize device connections and sessions so that all of your certificates are installed on your devices, and is done as rapidly as possible. But you can also manage the number of certificates provisioned during each provisioning operation using the Default Batch Setting when you configure your Bulk Provisioning job (from a minimum of 10 to a maximum of 1000 certificates).

You can easily view the status of jobs to see the results each time a job is run. You can then see the number of certificates and keys that were provisioned. Using the Trust Protection Platform log, you can review any errors that might have occurred so you can resolve them.

This section shows you how to create, run, and manage your Bulk Provisioning jobs.

Before you create and run a new bulk provisioning job

Before you configure a new bulk provisioning job, verify the following:

- Your administrator must load a PowerShell script for your device type into the `\Venafi\Scripts\AdaptableBulk\` folder on the Trust Protection Platform server.
- Make sure that you've correctly configured each device object in the Policy Tree.

For example, make sure each device object is configured with the correct host name (or IP address) of the device.

For more information about creating and configuring device objects, see [Device object settings \(agent and agentless\)](#) in the *Certificate Authority and Hosting Platform Integration Guide*.
- Make sure that your administrator has granted you the following permissions:
 - Read permission to the Bulk Provisioning Manager of at least one Trust Protection Platform engine (Platforms tree)
 - Read access to at least one device object
 - Write and Create access to a folder to create the job
 - Private key Read access to at least one folder containing valid certificates

Certificates are only applicable to bulk provisioning jobs if they are not disabled and they have a private key stored.

DID YOU KNOW? The management type of a certificate does not factor into whether a certificate can be installed by a bulk provisioning job. Job options allow you to control whether expired, revoked, or previous versions of certificates are installed.

For more information, see [Assigning permissions to an object in Policy Tree](#) in the *Venafi Trust Protection Platform Administration Guide*.

Creating a new Bulk Provisioning job

From the Jobs list view in Aperture, you can create a new bulk provisioning job in the same way you create other types of jobs, such as network and onboard discovery jobs.

IMPORTANT Before you begin creating a new bulk provisioning job, carefully review the topic, ["Before you create and run a new bulk provisioning job"](#) above.

To create a new Bulk Provisioning job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.

(Optional) To filter the Jobs list by one or more specific job types, use the Job Type filter. See ["Filtering the Jobs list by job type" on page 104](#).

2. Click **+ Create New Job** to start the Create New Job wizard.
3. On the **Create New Job** page, click **Bulk Provisioning**, and then click **Start**.
4. On the **Details** page, click the **Parent Folder** list to select the folder where you want the new job to be created.

TIP The folder you select must be one for which you have *Create* permissions.

These are folders in the Policy tree in Policy Tree and under the Configuration menu in Aperture.

5. In the **Name** field, type a name for the new job.
6. (Optional) Complete the following fields:
 - a. In the **Description** field, type a description of the purpose of the job.

A clear description can help to provide context for other administrators who might need to manage the new job.
 - b. In the **Contacts** field, select which contacts who you want to receive notifications of events that occur that are related to your new job.

This is also an effective method of identifying who is responsible for the job.
7. Click **Next**.
8. On the **Targets** page, in the **Target** and **Source** fields, select at least one device (*target*) and folder (*source*).

TIP If you've not already created the device object, see the next step.

IMPORTANT The folders you select must have at least one certificate contained in them. Also, make sure that you have the correct permissions to the devices and folders you select, and that the settings on your device objects are correct. For more information, see ["Before you create and run a new bulk provisioning job" on the previous page](#).

9. (Conditional) If you haven't yet created device objects, click **Create New Devices** and then do one of the following:

- a. If you already have the required credential, click **Create New Device Only** and do the following:

- i. In the **Device Addresses** field, type one or more new device addresses.

TIP When working with many devices, you can copy and paste all of the addresses into this field at once, provided that you include commas between each address.

- ii. In the **Device Folder** field, begin typing the name of the folder where you want the devices placed and select a folder.
- iii. In the **Credential** field, begin typing the name of the credential to use and then select it.
- iv. When you're finished, click **Save**.

- b. If you haven't yet created devices or credentials, click **Create New Device and New Credentials**, and then do the following:

- i. In the **Device Addresses** field, type one or more new device addresses.
- ii. In the **Device Folder** field, begin typing the name of the folder where you want the devices placed and select the folder.
- iii. In the **Credential Name** field, type a unique name for your new credential.
- iv. In the **Credential Folder** field, begin typing the name of the folder where you want the devices placed and select the folder.
- v. In the **Password** fields, type a password twice to confirm, and then click **Save**.

10. Under **Options**, check and/or configure the items you want to enable.

- **Include certificates that expired in the last n days:** You might have a reason to include expired certificates. This lets you decide which expired certificates to include based on the number of days since the expiration.
- **Include revoked certificates:** In some cases, you might want to retain a copy of revoked certificates, such as with SSL decryption traffic inspections. This can be helpful because revocation can take time to take effect (e.g. 7 days or longer).
- **Include historical certificates:** Enable this option if you want to deploy older certificates because they are still in use, or because you need the previous version history.
- **Include certificates without private key:** Enable this option if you want to deploy certificates that do not have private keys.

- **Certificate batch size:** If you need to manage any possible limitations with the target device (and its associated API), you can limit the number of certificates that are provisioned to that device in a single operation.

The default batch size is 200 certificates; if you don't specify a different batch size, the default is used. You can set this value to a minimum of 10 certificates and a maximum of 1000 certificates.

11. When you're ready to continue, click **Next**.
12. On the **Occurrence** page, specify when you want the new job to run, and then click **Next**.
13. On the **Installation Settings** page, select the PowerShell script you want to use for this bulk provisioning job.
14. (Optional) If you want to enhance troubleshooting capabilities of your Adaptable Bulk Provisioning Adaptable 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 523](#) in the Adaptable Bulk Provisioning Adaptable Flow PowerShell script reference.

15. Complete the fields required by your PowerShell script, and then either click **Create & Run** to save your changes and run the job immediately, or click **Create Job** if you plan to run the job at a later time (or have scheduled it to run later).

In either case, the Jobs list view appears and you can then take additional actions on your new job.

DID YOU KNOW? You can troubleshoot and specify additional Bulk Provisioning Manager service module settings by logging into Policy Tree. For more information, see ["Viewing Bulk Provisioning log events in Policy Tree" on page 529](#) and ["Configuring Bulk Provisioning Manager service module settings" on page 528](#) in the *Certificate Management Guide*.

Using sample Adaptable Bulk Provisioning PowerShell scripts

When you install Trust Protection Platform, PowerShell reference samples for use with Adaptable Bulk Provisioning is included in the `\Venafi\Scripts\AdaptableBulk\Samples` folder.

NOTE Your administrator will need to copy them from the `\Samples` folder into the `\AdaptableBulk` folder for them to be visible when you run the Create New Job wizard.

You can use the reference samples to better understand how to configure your own scripts.

Reference samples are *fully-functional implementations* that let you use the Bulk Provisioning feature. You do not need to know anything about the PowerShell functions to begin using reference samples. However, you do need to complete a few prerequisites, copy your scripts (described above), and then restart IIS.

To use the Symantec SSL Visibility Appliance sample PowerShell script

1. Verify the following prerequisites:
 - a. Make sure you have network connectivity to the SSL Visibility appliance on port 443
 - b. Make sure you have an account with the permissions that are detailed for the Blue Coat driver.

For more information, see [Blue Coat permission requirements](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

- c. Make sure that you have a trusted certificate installed on the SSL Visibility appliance.

2. Work with your administrator to copy the *Symantec SSL Visibility Appliance.ps1* script from the `\Venafi\Scripts\AdaptableBulk\Samples` directory to the `\Venafi\Scripts\AdaptableBulk` directory.

IMPORTANT You must also copy the PowerShell script to all Trust Protection Platform servers that are utilized in enrollment, or that are hosting the web console.

3. Restart IIS on each instance of Trust Protection Platform so that Venafi Platform can discover the newly copied scripts.

For information about available PowerShell script functions, see "[PowerShell script reference for Adaptable Bulk Provisioning](#)" on the next page.

To use the Imperva MX sample PowerShell script

1. Verify the following prerequisites:
 - a. Make sure you have network connectivity to the Imperva MX appliance on port 8083.
 - b. Make sure you have an account with the permissions that are detailed for the Imperva MX driver that you completed the Imperva prerequisite configuration.

For more information, see [Imperva Permission Requirements](#) and [Imperva prerequisite configuration](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

- c. Make sure that you have a trusted certificate installed on the SSL Visibility appliance.

2. Work with your administrator to copy the *Imperva MX (WAF).ps1* script from the `\Venafi\Scripts\AdaptableBulk\Samples` directory to the `\Venafi\Scripts\AdaptableBulk` directory.

IMPORTANT You must also copy the PowerShell script to all Trust Protection Platform servers that are utilized in enrollment, or that are hosting the web console.

3. Restart IIS on each instance of Trust Protection Platform so that Venafi Platform can discover the newly copied scripts.

For information about available PowerShell script functions, see ["PowerShell script reference for Adaptable Bulk Provisioning"](#) below.

PowerShell script reference for Adaptable Bulk Provisioning

Venafi Adaptable Drivers utilize PowerShell scripts—one for each driver—that contain functions called during various stages of the certificate lifecycle. The Adaptable Bulk Provisioning scripts have only one function: *Install-Certificates*.

Similar to the Adaptable Application PowerShell script, a FIELD DEFINITIONS header in the Adaptable Bulk Provisioning script defines extra fields that allow a user to provide additional metadata to the script.

For additional information about Venafi Adaptable Drivers and using PowerShell scripts, see [About Venafi Adaptable Driver PowerShell scripts](#).

Variable Name	Data Type	Description
Certificate	Hash Table Array	Certificates to be provisioned in Base64 PEM format. Each certificate in the certificates array is a hash table that includes the following: ▪ Name: the certificate Common Name (if it exists) or a DNS SAN (if it exists), or an OU (if it exists); otherwise, the serial number ▪ Serial: the serial number of the certificate ▪ Thumbprint: the SHA1 thumbprint of the certificate ▪ ValidTo: the expiration date of the certificate as a <i>YYYYMMDD</i> string ▪ Certificate: the Base64-encoded X509 certificate PEM ▪ PrivateKey: the Base64-encoded, non-encrypted private key PEM

Variable Name	Data Type	Description
BulkJobDN	String	Contains the Trust Protection Platform distinguished name (DN) of the calling application object.
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
HostAddress	String	Contains the hostname or IP address specified by the device object.
TcpPort	Integer	A value containing the TCP port specified by the application object.

Variable Name	Data Type	Description
UserName	String	The user name portion of the user name or private key credential assigned to the device or application object. Used for authenticating with the device.
UserPass	String	The password portion of the user name credential assigned to the device or application object. Used for authenticating with the device.
UserPrivKey	String	The privacy-enhanced electronic mail (PEM)-formatted RSA private key portion of the private key credential assigned to the device or application object. Used for authenticating with the device via SSH.
VarBool1	Boolean	The value of the Yes/No (true/false) user-defined field as defined by the header at the top of the PowerShell script.
VarBool2	Boolean	The value of the Yes/No (true/false) user-defined field as defined by the header at the top of the PowerShell script.
VarPass	String	Contains the value of the password field as defined by the header at the top of the PowerShell script.
VarText1	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.
VarText2	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.
VarText3	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.
VarText4	String	The text contained in the user-defined field as defined by the header at the top of the PowerShell script.
VarText5	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	Specify "Success" to indicate the job completed normally and in a manner that should be considered successful. Specify any value other than "Success" (e.g. "Failed") to indicate the job completed but encountered problems. Fatal errors during execution of the script should be reported by throwing exceptions. Exception messages are captured in log events for the job. See "Viewing Bulk Provisioning log events in Policy Tree" on page 529.
RejectedCertificates	String Array	SHA1 thumbprints for certificates that could not be imported for expected reasons.
FailedCertificates	String Array	SHA1 thumbprints for certificates that could not be imported for unexpected reasons.

For information about processing stages, see ["About certificate lifecycle management"](#) on page 27.

About debug logging

When a user has requested debug logging by checking **Enable Debug Logging** for Adaptable FlowAdaptable Bulk ProvisioningAdaptable SSH Key Discovery, 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 FlowAdaptable Bulk Provisioning, see ["Creating a new Bulk Provisioning job"](#) on page 515.

Protecting against unapproved changes to Adaptable Bulk Provisioning 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.

When you encounter a PowerShell script error, you'll need to open the associated Adaptable Bulk Provisioning job in Aperture where you assigned the script and re-save the installation settings. When you do, the driver is re-enabled and you can run the job again.

To re-enable an Adaptable Bulk Provisioning driver following a change to its associated PowerShell script

1. Open and review the associated scripts to verify that they contain only approved changes.
2. In TLS Protect, select the associated Adaptable Bulk Provisioning job from the **Jobs** list, and then click **Details and Targets**.
3. At the bottom of the **Details and Targets** page, under **Installation Settings**, click **Edit Installation Settings**.
4. On the **Application Specific Settings** page, just click **Save**.
5. On the **Details and Targets** page, click **Run Now** to run the job again.

Editing an existing bulk provisioning job

If you need to change the settings for existing bulk provisioning jobs, you can edit and apply the settings from the Jobs list.

To edit a bulk provisioning job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
2. Click the job name of the job that you want to edit.
3. On the job's **Details** page, use the sidebar to modify settings.
4. When you finish making changes, click **Save**.

DID YOU KNOW? You can troubleshoot and specify additional Bulk Provisioning Manager service module settings by logging into Policy Tree. For more information, see ["Viewing Bulk Provisioning log events in Policy Tree" on page 529](#) and ["Configuring Bulk Provisioning Manager service module settings" on page 528](#) in the *Certificate Management Guide*.

Scheduling a bulk provisioning job

You can schedule a bulk provisioning job to run automatically based on your time preferences. You can define a schedule at the time you create a new job. But if you had set the schedule to Manually, you can simply edit the job to set up a schedule.

To schedule a job

1. From the [TLS Protect menu bar](#), click **Configuration > Jobs**.
2. In the **Jobs** list, click the job you want to schedule.
3. In the sidebar, click **Schedule**, and then do the following:
 - a. (Optional) If you don't want to set a recurring time to run the job, leave **Frequency** set to **Manually**.
 - b. If you want to set a recurring time, use the drop-down arrow to select the **Frequency**.

Remember that all times are local, that is, the time displayed is the OS clock time and is localized.

Installing (provisioning) lots of certificates and keys at one time

Run Time

Frequency *

Manually

Manually

Every Week

Every Month

Every Year

c. Fill in the **Day**, **Month**, and **Start Time**, as needed.

4. When you're done, click **Save**.

DID YOU KNOW? You can troubleshoot and specify additional Bulk Provisioning Manager service module settings by logging into Policy Tree. For more information, see ["Viewing Bulk Provisioning log events in Policy Tree" on page 529](#) and ["Configuring Bulk Provisioning Manager service module settings" on page 528](#) in the *Certificate Management Guide*.

Renaming a bulk provisioning job

You can change the name of any existing bulk provisioning job at any time. This can be helpful when you discover that an existing name is not descriptive or meaningful enough to other users. Or sometimes, IT policies changes can lead to needed updates.

To rename a bulk provisioning job

NOTE You need the **rename** permission to the bulk provisioning job, or this functionality won't be available to you.

1. From the SSH Protect menu bar, click **Configuration > Jobs**.
2. Locate the bulk provisioning job you want to change.
3. Click on the bulk provisioning job name to open the details page.
4. Hover your mouse pointer over the bulk provisioning job name until you see the name highlighted, and then click it.
5. In the **Rename** box, type the new name in the **New Name** field, and then click **OK**.

Object names may not contain the backslash \ or less-than sign < characters. Object names (including their path ancestors in the policy tree) must be fewer than 255 total characters.

DID YOU KNOW? You can troubleshoot and specify additional Bulk Provisioning Manager service module settings by logging into Policy Tree. For more information, see "Viewing Bulk Provisioning log events in Policy Tree" on page 529 and "Configuring Bulk Provisioning Manager service module settings" on the next page in the *Certificate Management Guide*.

Running a bulk provisioning job manually

You can run any job type manually at any time from the Jobs list view. This is helpful if you have not yet added a schedule to a job, or if you cannot wait for the next scheduled run.

To run a job manually

1. From the TLS Protect menu bar, click **Configuration > Jobs**.
2. In the **Jobs** list, highlight the job you want to run, and then click **Run Now** from the Quick Action list.

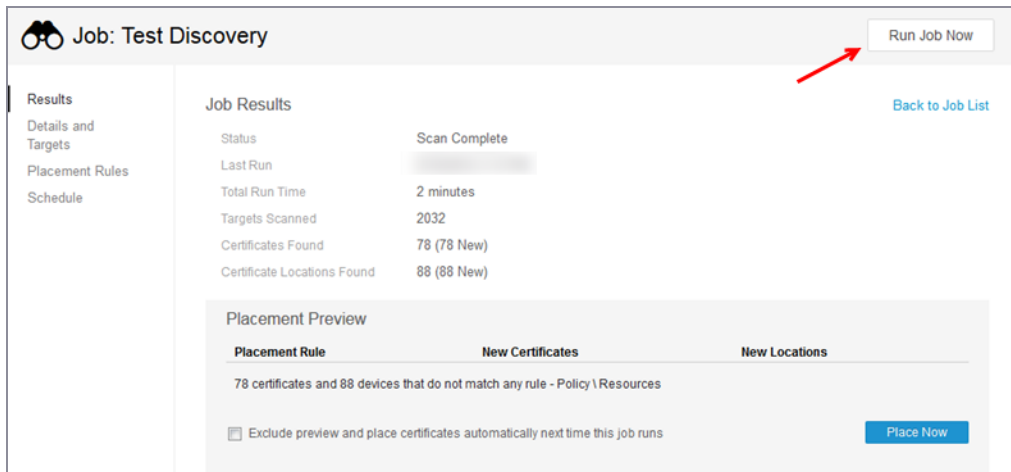
The screenshot shows the Venafi Jobs page. The top navigation bar includes 'VENAFI', 'Dashboards', 'Inventory', 'Jobs', 'Groups & Work', 'Reports', and 'Configuration'. A search bar and user profile are on the right. The 'Jobs' section has a '+ Create New Job' button and tabs for 'Network Discovery', 'Onboard Discovery', 'Bulk Provisioning', 'Placement Job', and 'TrustNet Discovery'. A table lists 18 jobs. The 'Run Now' buttons for the last four jobs are highlighted in a red box.

Job Name	Description	Next Run	Last Run	Type	Results	Status	Priority	Quick Action
Adaptable-OnboardDisco-AllApp	Onboard Discovery for all applications using the Venafi Adaptable driver	Manual	Never	Onboard Discovery	Certificates: 0	Canceling		Delete
CertDiscovery	Network Discovery job for finding certificates in SLC Office	1/30/2019 12:00 AM (-07:00 UTC)	1/23/2019 12:00 AM (-07:00 UTC)	Network Discovery	Certificates: 1 SSH Servers: 0	Scan Complete	1	Run Now
Day LIX Discovery		Manual	10/17/2017 9:17 PM (-06:00 UTC)	Network Discovery	Certificates: 0 SSH Servers: 0	Scan Complete	5	Run Now
dev-OnboardDisco-CAP1	CAP1 (SS Bindings)	Manual	Never	Onboard Discovery	Certificates: 0	Cancelled		Run Now
foobar	Adaptable	Manual	Never	Onboard Discovery	Certificates: 0			Run Now
MyBulkProvisioningJob001		Manual	Never	Bulk Provisioning	Certificates To Provision: 0 Provisioned Certificates via Full Run: 0 Provisioned Certificates via Express Run: 0			Run Now

OR

Installing (provisioning) lots of certificates and keys at one time

From the **Details and Targets** tab of a job, click **Run Now**.



Configuring Bulk Provisioning Manager service module settings

Bulk Provisioning jobs that have run successfully are triggered automatically when new certificates appear in the source folders you've specified in the jobs settings. This is also true when existing certificates are imported with their private keys.

In Policy Tree, you can specify the frequency (in seconds) with which the Bulk Provisioning Manager checks the source folders defined in existing bulk provisioning jobs. And like other Trust Protection Platform service modules, the Bulk Provisioning Manager can be enabled or disabled.

To configure Bulk Provisioning Manager service module settings

1. From the **TLS Protect** menu bar, click **Policy Tree**, then open the **Platforms** tree.
2. In the **Platforms** tree, select the device object where the Bulk Provisioning Manager service module is installed, and then click it.
3. From the **Bulk Provisioning Manager > Settings** tab, do the following:
 - a. (Conditional) If you want to enable (or disable) Bulk Provisioning Manager, select (or clear) the **Disable this module** check box.
 - b. In the **Express Run Interval** field, type (in seconds) how often Bulk Provisioning Manager should check the source folders configured in your bulk provisioning jobs for new certificates (enrolled or imported).

The default setting is 60 seconds.

- c. In the **Express Run Retry Interval** field, type (in seconds) how often Bulk Provisioning Manager should wait before retrying after a failed attempt.

Bulk Provisioning Manager retries five (5) times before putting a bulk provisioning job into a *failed* state.

The default setting is 60 seconds.

4. When you're finished, click **Save**.

DID YOU KNOW? To create, move, rename, or delete bulk provisioning work, log in to Aperture. For more information, see ["Creating a new Bulk Provisioning job"](#) on page 515 in the *Certificate Management Guide*.

Viewing Bulk Provisioning log events in Policy Tree

When you need to view events specific to Bulk Provisioning—for example, when you're troubleshooting—take a look at the log found on the Bulk Provisioning job object in the Policy tree.

You can also access logged events on the Bulk Provisioning Manager object in the Platforms tree.

To view log events for Bulk Provisioning (Policy tree)

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. In the **Policy** tree, find the your Bulk Provisioning job object click it.
3. Review logged events on the **General > Log** tab.

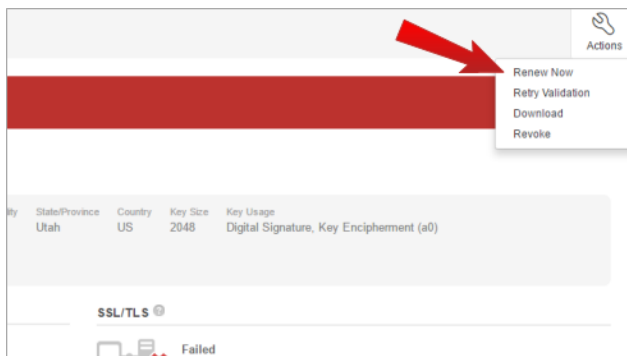
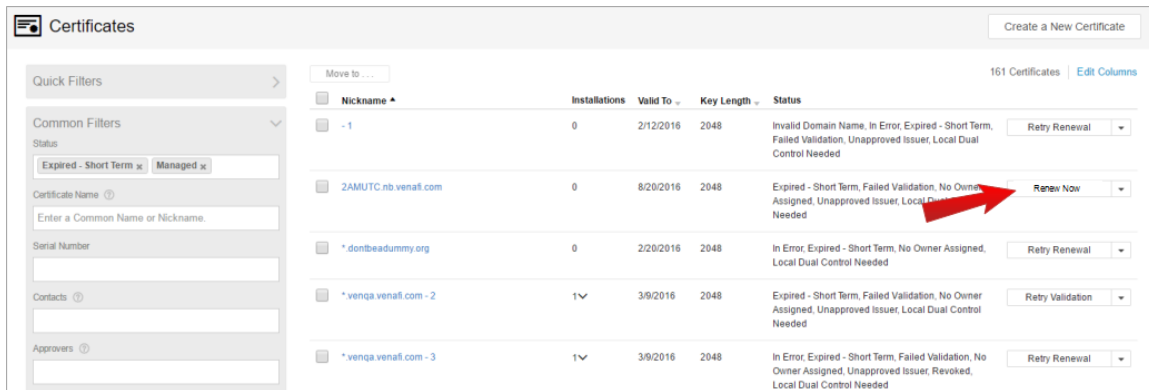
DID YOU KNOW? To create, move, rename, or delete bulk provisioning work, log in to Aperture. For more information, see ["Creating a new Bulk Provisioning job"](#) on page 515 in the *Certificate Management Guide*.

Renewing a certificate manually

The Renew Certificate wizard walks you through identifying the certificate and specifying its location.

To renew a certificate

1. Find the certificate you want to renew.
2. You can use filters to help narrow your search.
3. In the certificate list, click **Renew Now** or in the certificate's detail page, click **Actions** > **Renew Now**.



4. Review the **Requested Renewal Details**.

Requested Renewal Details

CERTIFICATE REQUEST DETAILS

Certificate Folder

Policy\North America

Nickname

cert-100-1024-SHA1-RSA-42-3

Management Type

Provisioning

Contacts

admin

Hash Algorithm

SHA-256

CSR Generation

Generate a CSR for me

Common Name

cert-100-1024-SHA1-RSA-42-3

Organization

Venafi

Key Strength

2048

Approvers

admin

Automatic Renewal?

No

Certificate Authority

Policy\North America\Eng\MCSA

Edit and Renew

Cancel

Renew

5. Do one of the following:
- If no changes are needed, click **Renew**.
 - If you need to make changes, click **Edit**, and then edit the Renewal Details.
 - When you're done, click **Submit**.

In the certificate list, the state changes to **Renewing**.

Installation statuses explained

On the **Installations** page, here is an explanation of what each Installation status means.

installing.test.nb.venafi.com			
Policy\Policy For Install Tests\hrserver.venafi.com\			
Overview			
Certificate Locations	2 locations		
Permissions			
	Application	Device	Installation Status
	Web Server for HR IIS6	hrserver.venafi.com 192.168.3.44	In Error
	P12 PKCS#12	hrserver.venafi.com 192.168.3.44	Approval Scheduled

State	What It Means
Not Validated Yet	Validation is enabled but hasn't been performed on this installation yet.
In Error	An error occurred during the installation process. Clicking  will give you details about the problem and solutions for fixing it.
Disabled	The installation is disabled. No installation, validation, or licensing count takes place.
Queued for Install	Installation has been initiated and is waiting to start.
Installing	The certificate is being installed.
Approval Scheduled	The installation has been approved and is scheduled to occur at a specific date and/or time.
Pending My Approval	The user who is currently logged in needs to approve the installation.
Pending Someone Else's Approval	Someone other than the current user needs to approve the installation.
Installation Validation Successful	Validation completed successfully.
Installation Validation Failed	Validation was not completed successfully. Clicking  will give you details about the problem and offer solutions for fixing it.
Installation Validation Disabled	Validation is disabled.
Validating	Certificate is in the process of being validated.
Validation Not Supported	Certificate installation was performed by an Agent. Validation must be done manually.

Validating a certificate's installation (onboard validation)

Onboard validation (called *installation validation* in Aperture) is a process by which Trust Protection Platform verifies that a certificate is properly installed, and that that certificate's settings comply with the settings configured on the certificate object in Trust Protection Platform.

Onboard validation determines if the Application object's configuration is correct and verifies that the correct certificate is installed on the server. If Trust Protection Platform can locate the certificate, it knows the Application object's certificate configuration is correct. Finally, when Trust Protection Platform retrieves the certificate serial number, it can determine if the correct certificate is installed.

NOTE Onboard validation applies to application objects only.

Unless you disable it, onboard validation occurs each time a certificate is automatically renewed and installed. To learn how to disable onboard validation, see ["Disabling SSL/TLS validation "](#) on page 554.

How does it work?

Certificate installation verification	
What it verifies	▪ Application objects only
What it's looking for	▪ Application object has correct configuration ▪ Correct certificate is installed on the server
How it works	▪ If Trust Protection Platform authenticates with the server, then it knows the Application object's credentials are correct. ▪ If Trust Protection Platform locates the certificate, it knows that the Application object's certificate configuration is correct.

Onboard validation can be done using agentless connections, or by using the Trust Protection Platform Server Agent.

You can see the validation status on the certificate's details page.

Validation Status

The validation status is displayed on the certificate details screen in the **Validation** section.

VALIDATION ?



SSL/TLS: **Success**
 Installations: **No validation results**
 6/18/2019 10:01 AM (+03:00 UTC)

This box contains the following information:

- **Timestamp.** This indicates when the validation check was last performed. This may be updated either by daily tasks, or by kicking off a manual validation for a certificate via either the WebSDK or by clicking the **ValidateNow** option in the **Actions** button.
- **SSL/TLS.** This shows either *Success* or *Failure*, if after reviewing all the validation details for SSL/TLS validation if everything is successful, the result will be *Success*. If anything fails with the End Entity or Chain validation, then the result will be *Failure*.
- **File/Installation.** This checks the onboard/file/installation validation of all provisioning applications. If all are successful, then this will show *Success*. If any fail, then this will be shown as a *Fail*. If all provisioning applications are basic applications, then this will show *No validation results*.
- **State.** The state is represented by the icon. This state shows the overall validation status of the certificate. If both SSL/TLS and File/Installation validation types are successful, this will show *Success*. If either SSL/TLS OR File/Installation validation types failed, this will show *Fail*.

To kick off an instant validation of both SSL/TLS and File/Installation validation, click the **Validate Now** option in the Actions button.

Validation Status in the Policy Tree

In the Policy Tree, the validation status is displayed on the Certificate **Summary** tab, in the **Certificate Status** panel.

Validation

Last Check: **6/18/2019 10:00:39 AM** SSL/TLS Result: **Success**
 State: **Success** File Result:

This box contains the following information:

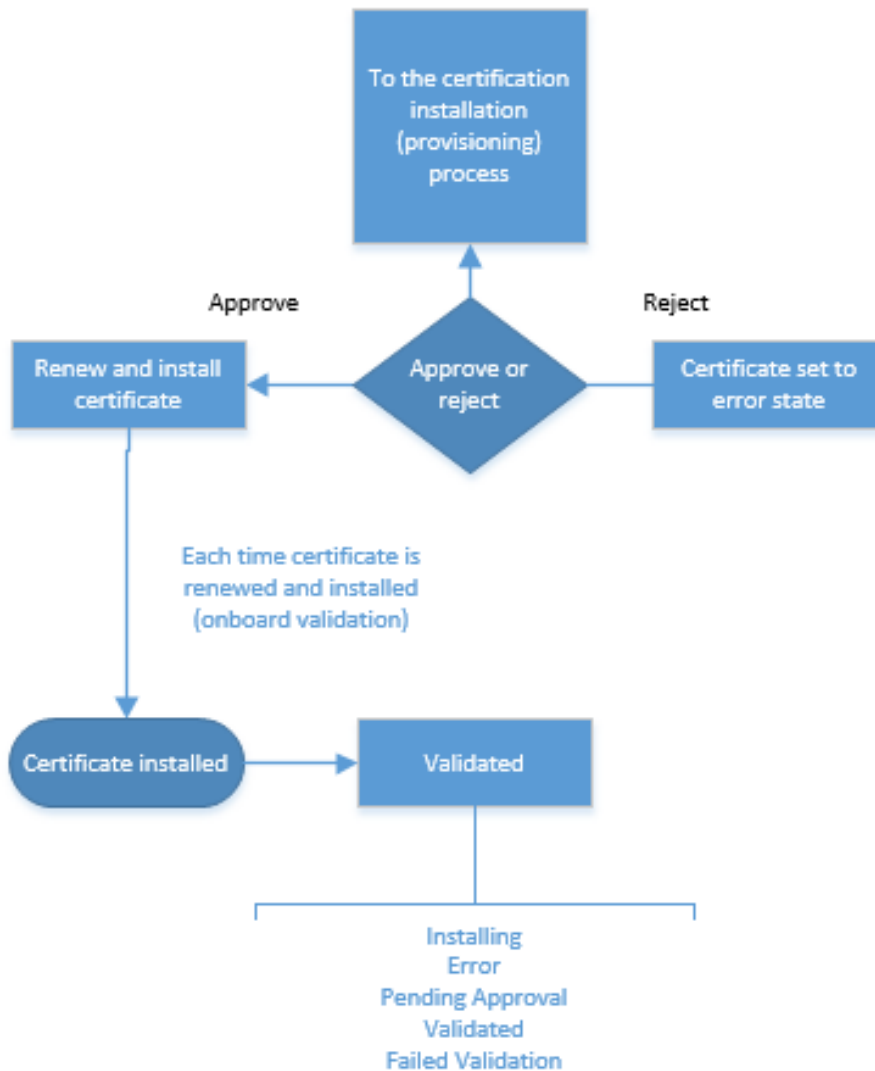
- **Last Check.** This indicates when the validation check was last performed. This may be updated either by daily tasks, or by kicking off a manual validation for a certificate via either the WebSDK or by clicking the **ValidateNow** button.
- **SSL/TLS Result.** This shows either *Success* or *Failure*, if after reviewing all the validation details for SSL/TLS validation if everything is successful, the result will be *Success*. If anything fails with the End Entity or Chain validation, then the result will be *Failure*.
- **File Result.** This checks the onboard/file/installation validation of all provisioning applications. If all are successful, then this will show *Success*. If any fail, then this will be shown as a *Fail*. If all provisioning applications are basic applications, then this will be blank.
- **State.** In Policy Tree, it is shown as the **State** field. This state shows the overall validation status of the certificate. If both SSL/TLS and File/Installation validation types are successful, this will show *Success*. If either SSL/TLS OR File/Installation validation types failed, this will show *Fail*.

To kick off an instant validation of both SSL/TLS and File/Installation validation, click the **Validate Now** button.

Validation of a certificate's installation (agentless)

For agentless connections, onboard validation occurs after each certificate installation when Trust Protection Platform verifies that a certificate is properly installed, and that the settings configured for the certificate comply with the settings for the certificate object Trust Protection Platform.

In the approval workflow for an agentless configuration of onboard validation, the validation occurs last:



To learn about onboard validation statuses, see "Review validation results" on page 548.

To learn how to disable onboard validation, see "Disabling SSL/TLS validation " on page 554

Validation of a certificate's installation (Server Agent)

For a Server Agent-based implementation, onboard validation works differently than when using agentless connections. Unlike agentless, agent-based onboard validations require that you manually request an onboard validation.

The Server Agent supports onboard validation using the following Venafi application drivers:

- PEM
- JSK
- PKCS#12
- CAPI
- IBM GSK

Before requesting onboard validation using the Server Agent, you must first complete the following prerequisites:

- Create the application object on a device that has the Provisioning Mode set to "Agent"
- Assign certificate installation work to an agent's group (and make sure the work is enabled)
- Fill out required application object fields

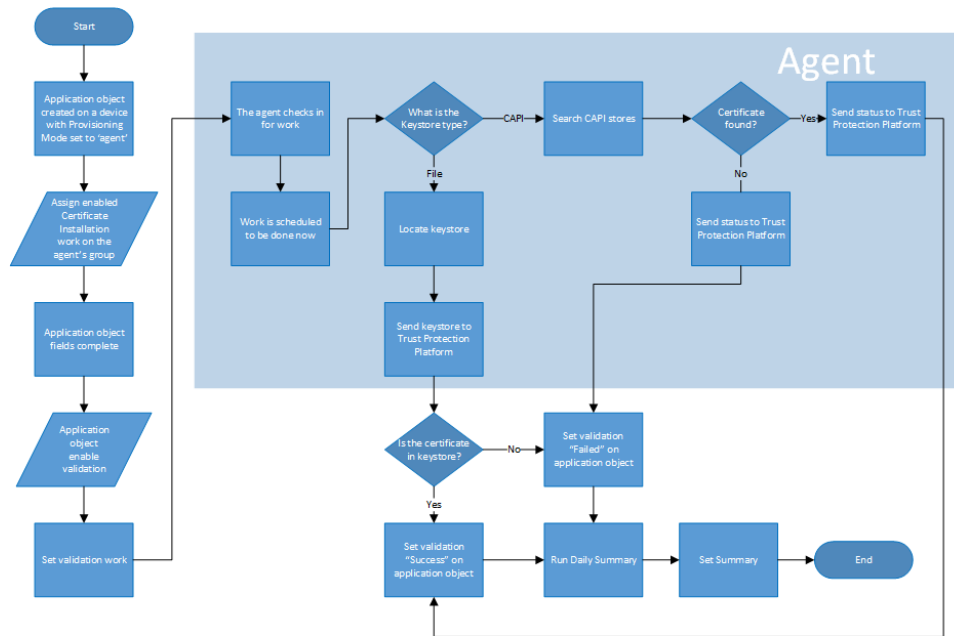
In order for PKCS#12 applications to perform agent-based onboard validation, you must fill out the Private Key Credential field.

- Enable validation on the application object

Server Agent-based Installation validation is initiated by Trust Protection Platform following provisioning and is done every night, as well as on demand.

The Server Agent performs the validation as part of the installation and validation work interval set on the work object. The overall validation of a certificate is updated each day during validation processing.

The following diagram shows the basic workflow when using Server Agent with onboard validation:



To learn about onboard validation statuses, see "Review validation results" on page 548.

To learn how to disable onboard validation, see "Disabling SSL/TLS validation " on page 554

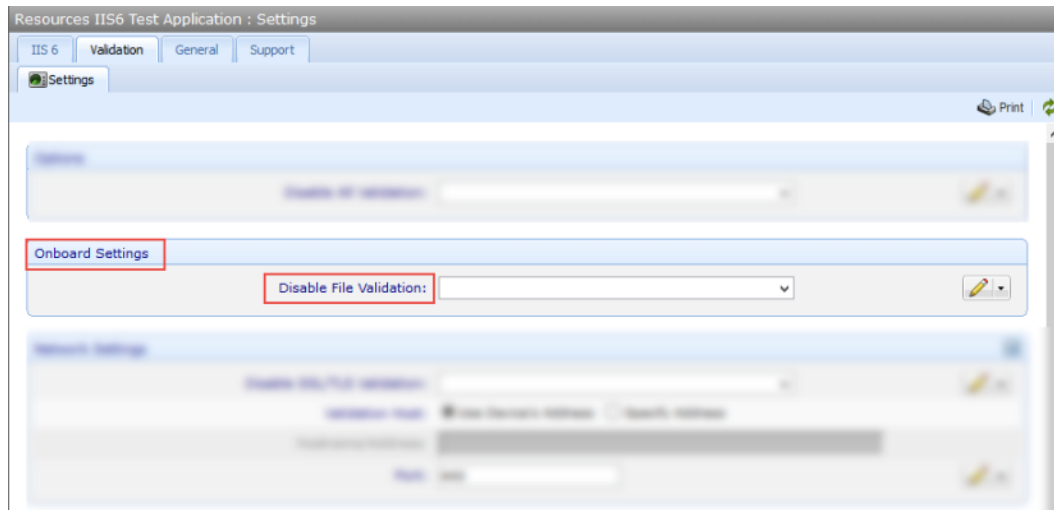
Disabling onboard validation

By default, onboard validation is *on*. You can disable it using the Policy Tree

To disable onboard validation

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. In the Policy tree, find the application for which you want to disable validation.
3. Click the **Validation** tab.
4. From the list, select **Yes** for the types of validation that you want to disable.

5. When you're done, click **Save**.



13

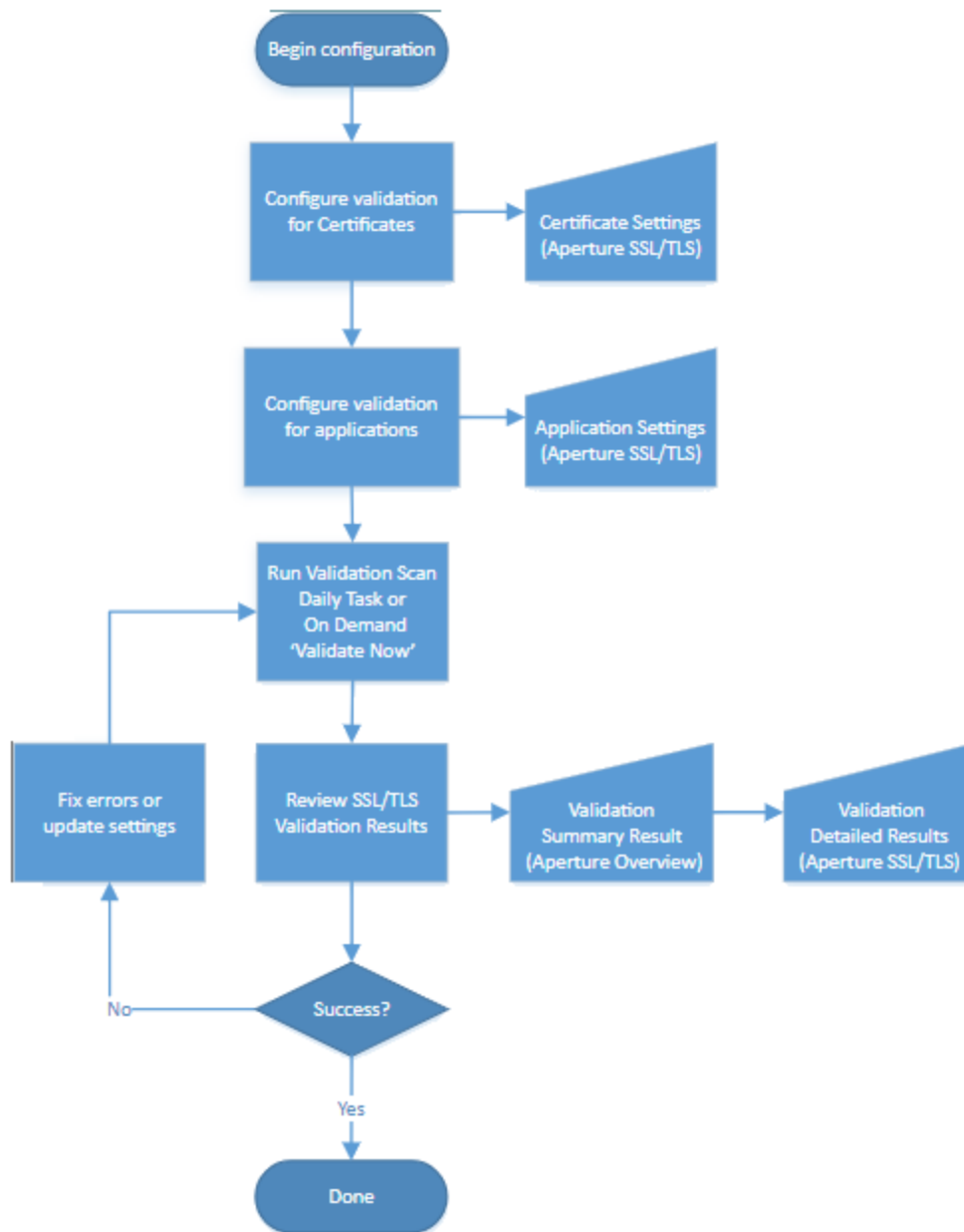
SSL/TLS network validation

The Venafi Trust Protection Platform™ validation feature validates your encryption system certificates and applications to determine if the correct certificate is being used. It also determines if it is functional and if it is installed in the correct place on its associated platform or keystore.

Security, compliance, and technological innovation have introduced new criteria for the validation of certificates and the servers that host them.

Trust Protection Platform offers certificate validation that is easy to use, provides more actionable results, helps assure compliance with industry standards, and supports best security practices.

- You can configure validation and see results in TLS Protect.
- When you view validation results, you can clearly see every target that was scanned for the certificate.
- Validation provides complete, qualitative analysis of the certificate chain presented by the hosting server.
- Validation identifies the SSL or TLS protocols that the hosting server supports. Venafi provides these communication protocols: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
- Different certificates that are hosted on the same IP address and port can be validated.



Network Validation

What it validates	SSL/ TLS application objects and certificates
What it's looking for	Certificate is functional

	Correct certificate is being used
How it works	If the server responds to SSL/TLS request, Trust Protection Platform knows the certificate is functional. When certificate's serial number is retrieved and compared, Trust Protection Platform can determine if the correct certificate is being used. If Use Certificate Common Name is enabled, Trust Protection Platform does a DNS lookup of the certificate's common name then validates the certificate at every IP address returned. Results are reported individually. If you enable Network Validation on the Application object, Trust Protection Platform validates the certificate associated with the Application object.

This chapter contains the following topics:

About configuring validation.....	544
Server name indication (SNI) support for validation.....	545
Supported certificate ciphers for network validation.....	545
Configuring validation for certificates.....	545
Configuring validation for applications.....	546
Running validation scans.....	547
Review validation results.....	548
Disabling SSL/TLS validation.....	554

About configuring validation

Validation has been a standard feature of Trust Protection Platform for many years. Validation is now easier to use, provides more actionable results, helps assure compliance with industry standards, and supports security best practices.

By default, validation scans run every day unless you disable validation.

To learn how to disable Network Validation, see ["Disabling SSL/TLS validation "](#) on page 554.

About configuring validation on the Policy Tree

To enable the validation feature on your Trust Protection Platform server, the Validation Manager module must be enabled in the Platforms tree. The Validation Manager is the engine that runs network validations on configured certificates and applications, and also runs onboard validations for applications.

If you selected **Validation** in the Component Selection window during the Trust Protection Platform installation, the Validation Manager module is enabled. If you did not select the validation component during installation, you must go to the Platforms tree and enable the Validation Module before you can run Network or onboard validations.

Validation Manager daily scans

The Validation Manager runs daily validation scans according to the daily task schedule configured on the Trust Protection Platform server object in the Platforms tree. You can configure the Trust Protection Platform server's Daily Task schedule to manage when the Validation Manager performs its daily validation scans.

NOTE The Trust Protection Platform server's Daily Task schedule also manages when Trust Protection Platform runs its Certificate monitoring scan.

For more information on configuring the Validation Manager module or Trust Protection Platform Server object, see [Configuring the Validation Manager Module](#) in the *Venafi Trust Protection Platform Administration Guide*.

Server name indication (SNI) support for validation

Validation sends hostnames or FQDNs, where applicable, as the *server name indication* (SNI) for TLS connections during network validation. Certificates can be validated in the case where more than one certificate is being hosted on the same IP address and port.

Supported certificate ciphers for network validation

Trust Protection Platform currently uses .NET for Network Discovery and Network Validation. The list of cipher suites that Trust Protection Platform supports is equivalent to what .NET running on the Windows host supports.

NOTE Ciphers can be enabled or disabled by the system administrator.

To learn more about supported cipher suites, visit <https://msdn.microsoft.com/en-us/library/windows/desktop/aa374757%28v=vs.85%29.aspx>.

Configuring validation for certificates

You can configure certificate validation in TLS Protect. As part of validation, you need to specify the certificate's validation settings so that Trust Protection Platform can locate the certificate and verify that it's installed correctly.

IMPORTANT You must have *View* and *Write* permissions to the application.

To configure certificate validation

1. From the **TLS Protect** menu bar, click **Inventory > Certificates**.
2. Find the certificate that you want to configure, and then click the certificate's name.
3. In the sidebar, click **SSL/TLS**.
4. Click **Certificate Settings**.
5. Edit the **Certificate SSL/TLS Validation Settings** as needed.

What each setting means

- **Validate SSL/TLS connections for this certificate?** Select **Yes** or **No**. Yes will enable Trust Protection Platform to turn on daily TLS validation of this certificate. The **Port** is the network port that Trust Protection Platform will use to connect to the target device hosting the certificate when making the TLS connection.
- **Use certificate's Common Name** - Validation scans include network addresses resolved from the common name of the certificate.
- **Use Certificate DNS Subject Alternative Names** - Validation scans include network addresses resolved from the DNS Subject Alternative Names (SANs) of the certificate, if any.
- **Validate the chain returned by the hosting server** - The chain returned by the hosting server is compared to the chain that Trust Protection Platform builds using its internal algorithm to ensure a match. By default, chain validation is enabled and affects the SSL/TLS validation result.
- You can define other network addresses and ports by creating a device and Basic application object.

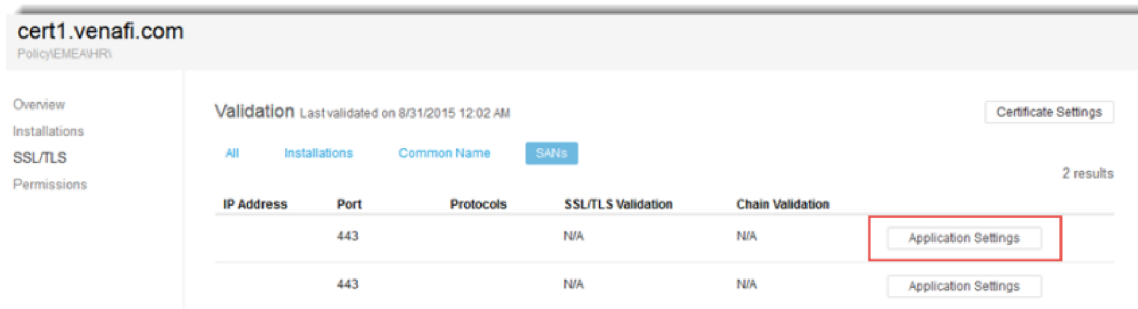
See [Creating a device object in Policy Tree](#).

Configuring validation for applications

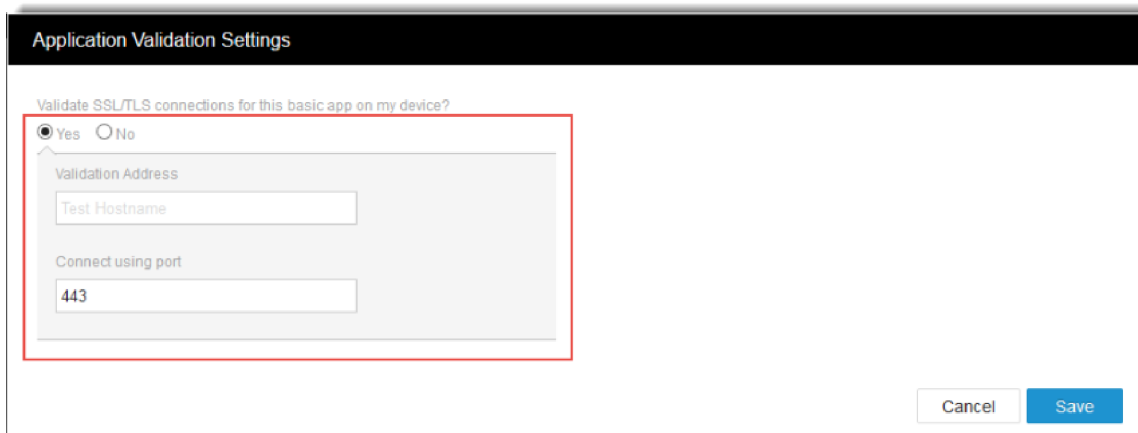
When you enable and configure validation on an application, Trust Protection Platform validates the certificate associated with the application.

To configure application validation

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. Find the certificate that is associated with the application.
3. Click the certificate's name.
4. In the sidebar, click **SSL/TLS**.
5. Click **Installation Settings**.



6. In the **Installation Validation Settings** dialog box, select **Yes**.
7. (Optional) Enter the **Validation Address**.
8. Enter the **Port** number.



9. Click **Save**.

Running validation scans

By default, validation scans occur daily according to the daily task schedule configured on the Trust Protection Platform server object in the Platforms tree. However, you can also manually run a validation scan.

Trust Protection Platform runs a validation whenever a certificate is automatically renewed and installed. This is called *SSL/TLS validation*.

To run a manual validation scan

1. From the Aperture menu bar, click **Inventory** > **Certificates**.
2. Find the certificate that you want to validate.
3. Click the certificate's nickname.
4. On the certificate's details page, click **Actions** > **Validate Now**.

When you click **Validate Now**, it triggers validation of the certificate and all of its installations.

The Validation statuses change to *In Process*.

The page automatically refreshes when the validation is complete.

5. To see more detailed validation results, switch to the **SSL/TLS** tab on the left.

To see what each validation result means, see "[Review validation results](#)" below.

Review validation results

When you enable network or onboard validation, Venafi Trust Protection Platform™ runs daily validation checks and reports the results.

In addition to reporting validation results on an application or certificate, Trust Protection Platform generates a validation error event if a certificate fails the validation test.

NOTE If validation is disabled for an object (either directly, or via policy) any existing validation data will be removed from the database on the next validation scan.

Validation Status

The validation status is displayed on the certificate details screen in the **Validation** section.

VALIDATION ?



SSL/TLS: Success
Installations: No validation results
6/18/2019 10:01 AM (+03:00 UTC)

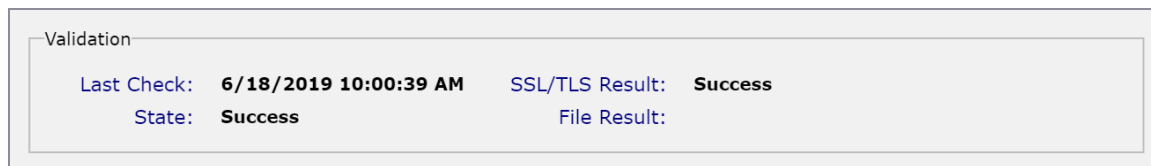
This box contains the following information:

- **Timestamp.** This indicates when the validation check was last performed. This may be updated either by daily tasks, or by kicking off a manual validation for a certificate via either the WebSDK or by clicking the **ValidateNow** option in the **Actions** button.
- **SSL/TLS.** This shows either *Success* or *Failure*, if after reviewing all the validation details for SSL/TLS validation if everything is successful, the result will be *Success*. If anything fails with the End Entity or Chain validation, then the result will be *Failure*.
- **File/Installation.** This checks the onboard/file/installation validation of all provisioning applications. If all are successful, then this will show *Success*. If any fail, then this will be shown as a *Fail*. If all provisioning applications are basic applications, then this will show *No validation results*.
- **State.** The state is represented by the icon. This state shows the overall validation status of the certificate. If both SSL/TLS and File/Installation validation types are successful, this will show *Success*. If either SSL/TLS OR File/Installation validation types failed, this will show *Fail*.

To kick off an instant validation of both SSL/TLS and File/Installation validation, click the **Validate Now** option in the Actions button.

Validation Status in the Policy Tree

You can also view the validation status in the Policy Tree, where it is displayed on the Certificate **Summary** tab, in the **Certificate Status** panel.



This box contains the following information:

- **Last Check.** This indicates when the validation check was last performed. This may be updated either by daily tasks, or by kicking off a manual validation for a certificate via either the WebSDK or by clicking the **ValidateNow** button.
- **SSL/TLS Result.** This shows either *Success* or *Failure*, if after reviewing all the validation details for SSL/TLS validation if everything is successful, the result will be *Success*. If anything fails with the End Entity or Chain validation, then the result will be *Failure*.

- **File Result.** This checks the onboard/file/installation validation of all provisioning applications. If all are successful, then this will show *Success*. If any fail, then this will be shown as a *Fail*. If all provisioning applications are basic applications, then this will be blank.
- **State.** In Policy Tree, it is shown as the **State** field. This state shows the overall validation status of the certificate. If both SSL/TLS and File/Installation validation types are successful, this will show *Success*. If either SSL/TLS OR File/Installation validation types failed, this will show *Fail*.

To kick off an instant validation of both SSL/TLS and File/Installation validation, click the **Validate Now** button.

Example of detailed results

The certificate's SSL/TLS page lists the results of network validation for addresses provided by the certificate's Common Name, DNS Subject Alternative Names, and its installations. Results of SSL/TLS validation, chain validation, and protocol detection are presented here for each address and port that were validated.

protocols	SSL/TLS Validation	Chain Validation
SSL 1.0, TLS 1.1, TLS 1.2	Match but not current	Mismatched chain
SSL 1.0, TLS 1.1, TLS 1.2	Match but not current	Mismatched chain
SSL 3.0, TLS 1.0	Match but not current	Mismatched chain
	Host not resolved	N/A
	Host not resolved	N/A
	Host not resolved	N/A

SSL/TLS Validation Results

Validation Result	Description
Hostname not resolved	Hostname is not resolvable into a network address using DNS.
Connection failure	Unable to establish a network connection with the hosting device. This may be due to it being offline, being blocked by a firewall, or a misconfiguration that directed Trust Protection Platform to the wrong place (e.g. wrong port).
Host did not present a certificate	Target is listening on the port but didn't present a certificate.
Old version found	Target presented a certificate that matches one that is in history.
Unexpected certificate found	Target presented a certificate that matches one in inventory but not in history.
Unmanaged certificate found Also: Mismatch with Unknown (in the Policy Tree)	Target presented a certificate that doesn't match any certificates in inventory or history.
Validation not supported	Network validation is not supported by the application object (Imperva, Tealeaf PCA, Connect:Direct, etc.).
Disabled	Network validation is disabled for an application object.
Setting Error	Required information has not been entered into the Trust Protection Platform.

Validation Result	Description
Host is unreachable	Unable to establish a network connection with the hosting device. This may be due to it being offline, being blocked by a firewall, or a misconfiguration that directed Trust Protection Platform to the wrong place.
No Local Certificate	A certificate object exists but no X509 certificate is stored in the database.
Unknown error	Trust Protection Platform encountered an error but could not identify it.

Chain Validation Results

Per the guidelines outlined in [RFC5246](#), a certificate chain that includes only a root and a leaf certificate can still be deemed valid even if only the leaf certificate is presented.

Validation Result	Description
No chain found	No chain was returned by the endpoint.
Invalid chain	The chain returned by the endpoint cannot be used to form a valid chain.
Incomplete chain	The chain returned by the endpoint did not include a sufficient number of intermediate certificates to build a complete chain anchored by a root CA.
Chain expiring soon	One or more of the CA certificates expires before the end-entity does.
Blacklisted chain	One or more of the CA certificates is blacklisted by the Roots tree.
Mismatched chain	The chain returned by the endpoint does not match the one constructed by the Trust Protection Platform chain building algorithm.

Validation Result	Description
Chain building failed	Trust Protection Platform's chain building algorithm is missing one or more intermediate or root CA certificates and is unable to construct a complete chain. Add the missing certificate to the Root tree.
System busy, will retry	Trust Protection Platform could not start validation and will retry later.
Disabled	Validation is disabled.
Unknown error	Trust Protection Platform encountered an error but could not identify it.

Onboard Validation Results

Validation Result	Description
Authentication failure	Not able to log into the host using the credentials assigned to the device or application.
Host is unreachable	Target is unreachable or not listening on the port.
Access failure	Unable to read the certificate or certificate metadata due to permissions or missing asset.
Old version found	Target presented a certificate that matches one that is in history.
Unexpected certificate found	Target presented a certificate that matches one in inventory but not in history.

Validation Result	Description
Unmanaged certificate found	Target presented a certificate that doesn't match any certificates in inventory or history.
Disabled	Network validation is disabled for an application object.
Unknown error	Trust Protection Platform encountered an error but could not identify it.

Disabling SSL/TLS validation

You might want to disable SSL/TLS validation for one of the following reasons:

- the certificate is not presented on a network where it can be accessed by Trust Protection Platform (non-server certificate)
- there is no network connectivity between Trust Protection Platform and the server hosting the certificate
- to reduce the number of error notices that are generated when validation fails

You can disable SSL/TLS validation in two ways, either at the folder level or at the individual certificate level.

To disable SSL/TLS validation

At the folder level

1. From the **TLS Protect** menu bar, click **Configuration > Folders**.
2. Find the folder that you want to work with.
3. In the sidebar, click **Certificate Policy**.
4. In the **Validation Settings** section, under **Validate SSL/TLS connections for this certificate?**, select **No**.
5. When you're done, click **Save**.

For an individual certificate

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. Find the certificate that you want to work with.
3. On the certificate's details page, in the sidebar, click **SSL/TLS**.
4. In the **SSL/TLS Validation Settings** window, under **Validate SSL/TLS connections for this certificate?**, select **No**.
5. Click **Save**.

14

Implementing certificate workflow management

Venafi Trust Protection Platform™ allows you to integrate workflow management processes with its management of certificate lifecycles. Using workflow objects, you can require approvals or run SSH commands at stages of the certificate lifecycle. You can apply the workflows to an entire policy, or limit their action to only items associated with a specific application type such as a GSK keystore or Apache web server.

This chapter contains the following topics:

About workflows	558
About Adaptable Workflows	578
Managing approval requests in the Policy Tree	594
Managing certificate approval requests	596
About approval duration	599
About workflow approvers	601
Viewing pending approvers for a workflow	602

About workflows

Venafi Trust Protection Platform™ allows you to require approvals or run SSH commands at stages of the certificate lifecycle. You can apply workflows globally, or limit their action to only certificates associated with a specific application type such as a GSK keystore or Apache web server.

NOTE Trust Protection Platform is able to run local SSH commands only against the following applications: Apache, GSK, IIS5, iPlanet, JKS, PEM, PKCS#12, and Tealeaf PCA.

About Workflows in Trust Protection Platform

What are Trust Protection Platform workflows?

Application Workflows are defined in workflow objects, but applied using folders. Workflows and folders are created and managed in the Policy (Folder) tree. In the Policy tree hierarchy, workflow objects are created under their corresponding folders.

What can I do with workflows?

Workflows allow you to require one or more approvals or to run SSH commands at specific stages of the certificate lifecycle. You can apply workflows globally, or limit their action to only certificates associated with a specific application type such as a GSK keystore or Apache web server.

What prerequisites need to be met for approvals to work?

You need to make sure that you have enabled notifications in the system. If you have already enabled notifications for certificate or SSH work, you don't need to do this again, as this is a system-wide setting.

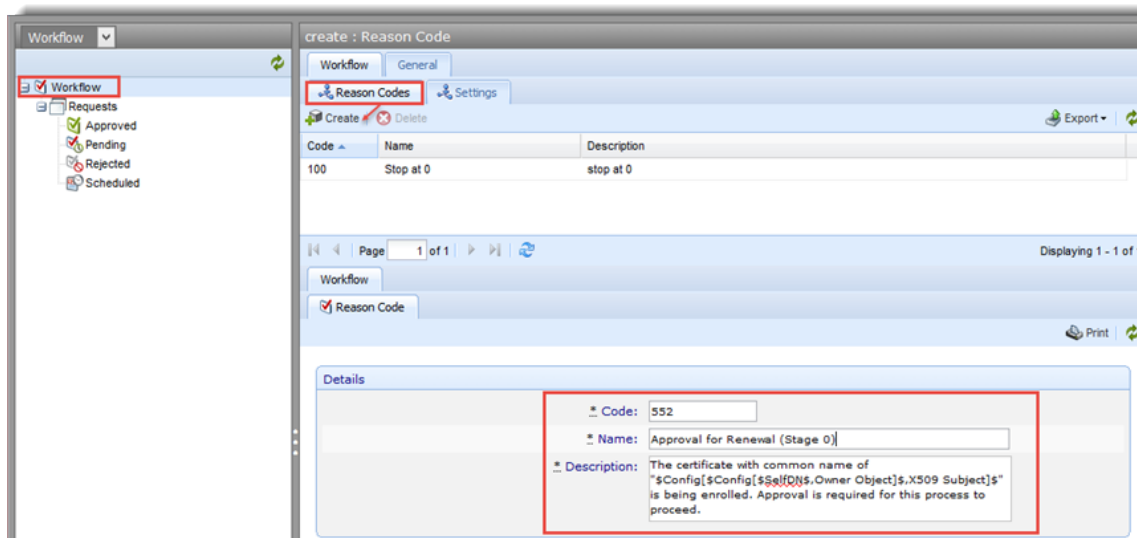
For details about enabling notifications, see ["Setting up notifications and logging" on page 429](#) in the Certificate Management Guide.

Where do Approval Reason Codes fit in?

When a workflow triggers an Approval Request, the approver receives a notification that includes the workflow's associated Reason Code. The Reason Code provides instructions or information for the workflow approvers.

Although Approval Reason Codes are selected in a Workflow in the Policy tree, the Reason Codes themselves are defined in the Workflow tree. You define the Approval Reason Codes that you want to reference in Workflow objects. The maximum Approval Reason Code value is 999.

For more information, see "Defining reason codes for certificate approvals" on page 573.

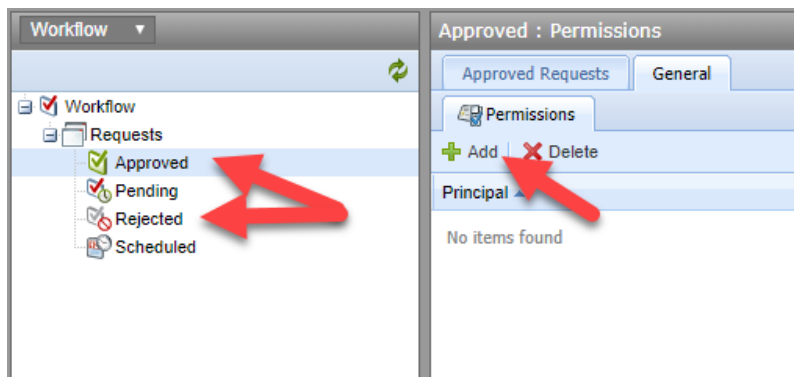


Workflow Approvals

The Workflow tree in the Policy Tree is also where approvers can view and manage Approval Requests. Approvers can see their own approved, pending, and rejected Approval Requests.

Approval Requests appear in the Workflow tree five minutes after they are triggered. Approvers can see only the approval requests that are assigned to them.

By default, only admins can see approved and rejected workflow objects. If you want other people in the organization to be able to see approved or rejected workflows, edit the Permissions settings for either the Approved or Rejected nodes in the Workflow tree.



Get Started: "Creating a certificate workflow" on the next page

Creating a certificate workflow

Workflow objects define the parameters required to implement a workflow approval or inject a local command at a specific stage of the certificate lifecycle.

You must have the *Create* permission to the policy where you want to create the workflow.

To create a Workflow object

1. From the [Platform menu bar](#), click Policy Tree.
2. Select the policy for which you want to create the workflow.
3. Click **Add > Workflow**.

The Detail View displays the Workflow's associated settings.

Add New : Workflow

Print

General

* Name:

Conditions

* If Stage is:

If Application or Trust Store is:

Actions

Inject Commands: ☐

Commands:

Commands will be evaluated for macros. If the command includes a single "\$", and is not intended to be used as a macro, then "\$" should be replaced with "\$\$."

Request Approval: ☐

Request Approval From: ☒ Approver assigned to object
☐ Specified approver
☐ Specify approver via macro

Specified Approver(s):

Approver Macro:

Approval Reason Code:

Save

4. In the **Name** field, enter a friendly name.

5. In the **Conditions** box, enter the qualifying conditions.

Setting	Description
If Stage Is	Enter the condition stage when the workflow event should be triggered. Stages are listed below.
If Application or Trust Store is	Will only trigger the approval if the certificate is installed on the Application or Trust Store selected from the list. If selected, this condition is in addition to the Stage Code. (That is to say there is an implied AND operation between the conditions.)

Certificate workflow Stage Codes

Certificate Stage Codes

Stage Code	Friendly Name	Description
0	StartProcessing	Prepares the certificate for lifecycle processing.
100	CheckStore	Applies only to remote generations. If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.
200	CreateConfigureStore	Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object.
300	CreateKey	Creates the private key.

Stage Code	Friendly Name	Description
DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400.		
400	CreateCSR	Creates the Certificate Signing Request (CSR). If Service Generated CSR is enabled and the certificate is associated with multiple applications, the CSR will be centrally generated so Trust Protection Platform can push the private key to multiple applications.
500	PostCSR	Submits the CSR to the Certificate Authority (CA). If you post a manual CSR, this is the first stage of the certificate lifecycle.
600	ApproveRequest	Approves the certificate renewal at the CA.
700	RetrieveCertificate	Retrieves the certificate from the CA.
800	InstallCertificate	Installs the certificate on the target application. This provisioning happens in several stages, such as 801, 802, etc. All stages between 800-899 are provisioning stages.
900	CheckConfiguration	Reserved for future use. You cannot apply this stage to a workflow.
1000	ConfigureApplication	Reserved for future use. You cannot apply a stage to this workflow.
1100	RestartApplication	Used for command injection workflow that must be executed after a certificate has been successfully provisioned.

Stage Code	Friendly Name	Description
1200	EndProcessing	Completes the certificate processing and, if configured, runs a Validation check on the certificate and application.
1400	Revocation	Submits a revocation request to the CA. Certificate revocation is a certificate operation; it does not involve the application driver.
1500	UpdateTrustStore	Updates the Trust Store at the host to comply with the effective bundle. To learn more, see " Viewing the Effective Bundle " on page 346.
1600	EndTrustStoreProcessing	Completes the processing of the Trust Store.

NOTE If there are multiple approvals set at the same stage, all approvals will trigger at the same time, and all approvals must be resolved before the workflow can continue. In Aperture, if a user is an approver for multiple workflow tickets at the same stage, approving or rejecting any of the workflow tickets will have the same effect on all workflow tickets assigned to the same object and stage.

6. In the **Actions** box, enter the appropriate actions.

Setting	Description
Inject Commands	Under the designated conditions, Trust Protection Platform executes the defined commands on the certificate's consumer application. Trust Protection Platform is able to run local SSH commands against the following applications: ◦ A10 AX Traffic Manager ◦ Apache ◦ F5 LTM Advanced ◦ IBM GSK ◦ Imperva MX ◦ JKS ◦ Layer 7 SSG ◦ Oracle iPlanet ◦ PEM ◦ PKCS#12 ◦ Tealeaf PCA Trust Protection Platform is able to run PowerShell commands over WinRM for the CAPI application. After Trust Protection Platform executes the command, the application driver logs an Inject Command Success or Inject Command Failure event so you can determine if the command successfully executed on the target application. The Inject Command Success event returns a value of zero (0) in the event's Value2 field. An Inject Command Failure event returns a non-zero numeric value in the Value2 field. To provide automatic notification for Inject Command Failure events, you can create a Notification Rule that triggers on a value greater than zero in the event's Value2 field. For more information, see "Creating notification rules" on page 432 in the <i>Venafi Trust Protection Platform Administration Guide</i>.
Request Approval	Check the box to request approval when this workflow condition is triggered.
Request Approval From	Select the source of the approver. ◦ Approver assigned to the object. For certificates, this is defined by the certificate settings in the Policy Tree.

Setting	Description
	◦ Specified approver. Hard-code the approvers to be used. Activates the Specified Approver(s) field where you must enter the identities used for the approval. If multiple approvers are added, all listed approvers must approve the workflow item before it will be approved. If any of the approvers rejects the workflow, the item will be rejected. ◦ Specify approver via macro. Allows you to enter a macro to dynamically select the workflow approver when the workflow is triggered. For more information on the Trust Protection Platform macro language, see the <i>Venafi Trust Protection Platform Macro Guide</i>. Activates the Approver Macro field where you must enter the macro command.
Approval Reason Code	Enter the Reason Code you want to include with the notification that is sent to the workflow approver. The maximum Approval Reason Code value is 999. IMPORTANT This option is required if you select Request Approval From. Approval Reason Codes also accompany customized explanations or instructions for workflow approvers. The drop-down list displays the Reason Codes defined in the Workflow tree. For more information, see "Defining reason codes for certificate approvals" on page 573.

7. Click **Save**.

IMPORTANT When you define a Workflow object that requires approval, you must also select an Approval Reason Code to provide explanations or instructions for the workflow approvers. To learn more, see ["Defining reason codes for certificate approvals" on page 573](#).

For a detailed description of the object settings, see ["Workflow object settings" below](#).

Workflow object settings

The following table describes the certificate workflow object settings.

Field	Description									
Conditions										
If Stage Is	Applies the workflow actions at the designated stage of the object lifecycle. The default lifecycle stages are as follows. Individual stages may vary per application. For information on certificate lifecycle stages for each application, see Protecting server platforms and keystores. If the private key and CSR are locally generated on the server, stages 0-700 are performed by the default X.509 Certificate Application driver. Stages 0-700 are only performed by the certificate’s consumer Application driver if the private key and CSR are remotely generated on the certificate’s consumer application. NOTE The private key and CSR are remotely generated on the certificate’s consumer applications if the Generate Key/CSR on Application option is enabled in the Certificate object.									
Certificate Stage Codes										
<table><tr><th>Stage Code</th><th>Friendly Name</th><th>Description</th></tr><tr><td>0</td><td>StartProcessing</td><td>Prepares the certificate for lifecycle processing.</td></tr><tr><td>100</td><td>CheckStore</td><td>Applies only to remote generations.</td></tr></table>		Stage Code	Friendly Name	Description	0	StartProcessing	Prepares the certificate for lifecycle processing.	100	CheckStore	Applies only to remote generations.
Stage Code	Friendly Name	Description								
0	StartProcessing	Prepares the certificate for lifecycle processing.								
100	CheckStore	Applies only to remote generations.								

Field	Description													
	<table><tr><th>Stage Code</th><th>Friendly Name</th><th>Description</th></tr><tr><td></td><td></td><td>If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.</td></tr><tr><td>200</td><td>CreateConfigureStore</td><td> Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object. </td></tr><tr><td>300</td><td>CreateKey</td><td> Creates the private key. DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400. </td></tr></table>		Stage Code	Friendly Name	Description			If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.	200	CreateConfigureStore	Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object.	300	CreateKey	Creates the private key. DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400.
Stage Code	Friendly Name	Description												
		If the private key and CSR are generated remotely, Trust Protection Platform compares the keystore or Directory configuration parameters specified in the Application object with the actual configuration on the application.												
200	CreateConfigureStore	Applies only to remote generations. If the certificate keystore does not exist, Trust Protection Platform creates the keystore as per the configuration parameters defined in the Application object.												
300	CreateKey	Creates the private key. DID YOU KNOW? Stage 300 is used for key generation only when the API of a target device separates keypair and CSR generation. When they're combined, both key and CSR generation are always done at stage 400.												

Field	Description		
	Stage Code	Friendly Name	Description
	400	CreateCSR	Creates the Certificate Signing Request (CSR). If Service Generated CSR is enabled and the certificate is associated with multiple applications, the CSR will be centrally generated so Trust Protection Platform can push the private key to multiple applications.
	500	PostCSR	Submits the CSR to the Certificate Authority (CA). If you post a manual CSR, this is the first stage of the certificate lifecycle.
	600	ApproveRequest	Approves the certificate renewal at the CA.
	700	RetrieveCertificate	Retrieves the certificate from the CA.
	800	InstallCertificate	Installs the certificate on the target application. This provisioning happens in several stages, such as 801, 802, etc. All stages between 800-899 are provisioning stages.

Field	Description	
	Stage Code	Friendly Name
	Description	
	900	CheckConfiguration
	Reserved for future use. You cannot apply this stage to a workflow.	
	1000	ConfigureApplication
	Reserved for future use. You cannot apply a stage to this workflow.	
	1100	RestartApplication
	Used for command injection workflow that must be executed after a certificate has been successfully provisioned.	
	1200	EndProcessing
	Completes the certificate processing and, if configured, runs a Validation check on the certificate and application.	
	1400	Revocation
	Submits a revocation request to the CA.	
	Certificate revocation is a certificate operation; it does not involve the application driver.	
	1500	UpdateTrustStore
	Updates the Trust Store at the host to comply with the effective bundle. To learn more, see "Viewing the Effective Bundle" on page 346.	
	1600	EndTrustStoreProcessing
	Completes the processing of the Trust Store.	

Field	Description												
If Application or Trust Store Is	Applies the workflow actions only to certificates installed on a specific type of application.												
Actions													
Inject Commands	Under the designated conditions, Trust Protection Platform executes the defined commands on the certificate's consumer application. Trust Protection Platform is able to run local SSH commands against the following applications: <table><tr><td>▪ A10 AX Traffic Manager</td><td>▪ Layer 7 SSG</td></tr><tr><td>▪ Apache</td><td>▪ Oracle iPlanet</td></tr><tr><td>▪ F5 LTM Advanced</td><td>▪ PEM</td></tr><tr><td>▪ IBM GSK</td><td>▪ PKCS#12</td></tr><tr><td>▪ Imperva MX</td><td>▪ Tealeaf PCA</td></tr><tr><td>▪ JKS</td><td></td></tr></table>	▪ A10 AX Traffic Manager	▪ Layer 7 SSG	▪ Apache	▪ Oracle iPlanet	▪ F5 LTM Advanced	▪ PEM	▪ IBM GSK	▪ PKCS#12	▪ Imperva MX	▪ Tealeaf PCA	▪ JKS	
▪ A10 AX Traffic Manager	▪ Layer 7 SSG												
▪ Apache	▪ Oracle iPlanet												
▪ F5 LTM Advanced	▪ PEM												
▪ IBM GSK	▪ PKCS#12												
▪ Imperva MX	▪ Tealeaf PCA												
▪ JKS													
	Trust Protection Platform is able to run PowerShell commands over WinRM for the CAPI application. After Trust Protection Platform executes the command, the application driver logs an Inject Command Success or Inject Command Failure event so you can determine if the command successfully executed on the target application. The Inject Command Success event returns a value of zero (0) in the event's Value2 field. An Inject Command Failure event returns a non-zero numeric value in the Value2 field. To provide automatic notification for Inject Command Failure events, you can create a Notification Rule that triggers on a value greater than zero in the event's Value2 field. For more information, see "Creating notification rules" on page 432 in the <i>Venafi Trust Protection Platform Administration Guide</i>.												

Field	Description
Request Approval From	Under the designated conditions, Trust Protection Platform submits an approval request to the workflow approver. You can request approvals for certificate renewals or workflow injection commands. The following options allow you to define the workflow approver.
Approver Assigned to Object	Defines a dynamic approver for the current Workflow object. Depending on which stage of the certificate lifecycle triggers the Workflow, Trust Protection Platform reads the workflow approvers from the certificate's Certificate object or consumer Application object or from the Certificate or Application tab of the certificate's parent Policy object. The rules for where Trust Protection Platform reads the workflow approver are as follows: ■ If the private key and CSR are locally generated on the Trust Protection Platform server and the workflow is triggered at stages 0-700 of the certificate lifecycle, Trust Protection Platform reads the approver from the Certificate object. At stages 800-1200, Trust Protection Platform reads the approver from the certificate's consumer Application objects. ■ If the private key and CSR are remotely generated on the certificate's consumer applications, Trust Protection Platform always reads the approver from the certificate's consumer Application objects. The private key and CSR are remotely generated on the certificate's consumer applications if the Generate Key/CSR on Application option is enabled in the Certificate object.

Field	Description
	For example, if the Workflow object is triggered at stage 100 of the certificate lifecycle and the private key and CSR are centrally generated, Trust Protection Platform reads the approver from the certificate's associated Certificate object. If the Workflow object is triggered at stage 800 of the certificate lifecycle, Trust Protection Platform reads the approver from the certificate's consumer Application objects.
Specified Approver	Defines a static approver for the current Workflow object. To select the workflow approvers: 1. In the Specified Approver(s) field, 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. IMPORTANT The group must be a Security group. 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 (*). 2. Select a Security Group Identity, and then click Select. Press Shift+click to select multiple, contiguous certificates. Press Ctrl+click to select multiple, discontinuous certificates. NOTE If you change the approver for an item that is pending approval, the update may take up to four hours to complete. Changing this setting can adversely affect performance of the system. If you need to change this setting contact Venafi Support.
Specify approver via macro	Allows you to enter a macro to dynamically select the workflow approver when the workflow is triggered.

Field	Description
	For more information on the Trust Protection Platform macro language, see the <i>Venafi Trust Protection Platform Macro Guide</i> .
Approval Reason Code	Reason Code you want to include with the notification that is sent to the workflow approver. The maximum Approval Reason Code value is 999. IMPORTANT This option is required if you select Request Approval From. Approval Reason Codes also accompany customized explanations or instructions for workflow approvers. The drop-down list displays the Reason Codes defined in the Workflow tree. For more information, see "Defining reason codes for certificate approvals" below.
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. For more information on the Log tab options, see General configuration options.
Permissions	On the object permissions tab, you select the users or groups you want to have 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 folder. If you configure Permissions in a parent object, those permissions are inherited by all subordinate objects.

Defining reason codes for certificate approvals

When a workflow triggers an approval request, the approver receives a notification that includes the workflow's associated reason code. The reason code provides instructions or information for the workflow approvers.

In the Workflow tree, you create the reason codes you want to associate with Certificate, or Injection Command Approval Requests. For example, you may define a general reason code that indicates the cost associated with approving the certificate, or you may create separate reason codes with specific instructions for each type of workflow that requires approval.

IMPORTANT You must have the *View* and *Write* permissions to the Workflow root.

Example: working with Reason Codes

Suppose you want to create reason codes for approving certificate approval and renewals. Here are some sample reason codes you could create.

Remember, you create your own reason code numbers.

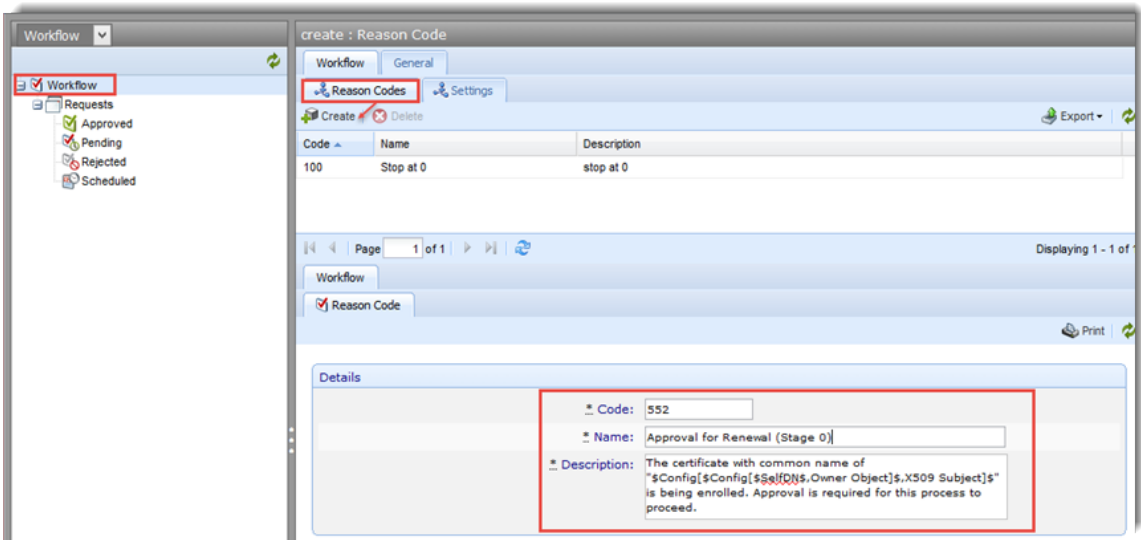
Reason	Description
Approval for Renewal (Stage 0)	The certificate with common name of "\$Config[\$Config[\$SelfDN\$,Owner Object]\$,X509 Subject]\$" is being enrolled. Approval is required for this process to proceed.
Approval for Enrollment (Stage 500)	The CSR for "\$Config[\$Config[\$SelfDN\$,Owner Object]\$,X509 Subject]\$" is waiting to be signed by the \$CN[\$Policy[\$Config[\$SelfDN\$,Owner Object]\$,Certificate Authority]\$\$\$ CA. Approval is required for this process to proceed.
Approval for Installation (Stage 800)	The certificate for the \$CN[\$Config[\$SelfDN\$,Owner Object]\$\$\$ application is now ready to be installed on the \$CN[\$ParentDN[\$Config[\$SelfDN\$,Owner Object]\$\$\$]\$\$\$ device. Approval is required for this process to proceed.
Approval for Service Restart (Stage 1100)	The certificate for the \$CN[\$Config[\$SelfDN\$,Owner Object]\$\$\$ application has been installed on the \$CN[\$ParentDN[\$Config[\$SelfDN\$,Owner Object]\$\$\$]\$\$\$ device, and the application is now pending a restart for the installation to be complete. Approval is required for this process to proceed.
Approval for Revocation (Stage 1400)	A request has been made to revoke a certificate which has a common name of "\$Config[\$Config[\$SelfDN\$,Owner Object]\$,X509 Subject]\$". Approval is required for this process to proceed.

To learn about Workflow stages, see "[Workflow object settings](#)" on page 565.

To learn about working with macros, see [Macro Overview](#).

To define a Reason Code

1. From the **Platform menu bar**, click Policy Tree.
2. Select the Root Workflow object.
3. Click **Create**.
4. Define the Reason Code settings.



The following table describes the Reason Code settings.

Field	Description
 Create	Creates a new Reason Code.
 Delete	Deletes the currently selected Reason Code.
 Export	Exports the Reason Codes to a CSV, tab-delimited, HTML, or XML file.
 Refresh	Refreshes the contents of the current page.
Code	Number you associate with the current Reason Code.

Field	Description
	You select this number when you include a Reason Code in an approval workflow. For more information, see " Approval Reason Code " on page 573.
Name	Reason Code name
Description	Reason Code text that displays in the notification that is sent to the approver. Reason Codes provide customized explanations or instructions for approvers. You can provide standard information such as the cost associated with approving the certificate or you may provide specific instructions for the certificate approval. You can include Trust Protection Platform macro commands in the Reason Code description. The macro language allows administrators to call variable content for fields such as message body and workflow approver.

5. Click **Save/Add**.

The Reason Code now appears in the Reason Code list and can be selected when you create certificate approval workflows.

Applying or blocking application workflows

The workflow applies to all subordinate Certificate and Application objects unless it is specifically blocked in a subordinate policy. When you block an inherited workflow, the workflow is blocked for all subordinate Certificate and Application objects.

To apply a workflow to the policy's subordinate Certificate and Application objects

1. Log in to Policy Tree.

IMPORTANT You must have the *View* and *Write* permissions to the policy where you want to apply the Workflow objects.

2. Select the **Policy** tree from the Tree drop-down menu.
3. In the Policy tree, select the Policy where you want to apply Workflow objects.
4. In the **Applied Workflows** group box, click **Add**.

5. Select the Workflow object you want to apply.
6. Click **Select**.
7. Click **Save/Apply**.

To block a workflow inherited from a Parent policy

1. Log in to Policy Tree.

IMPORTANT You must have the View and Write permissions to the Policy where you want to apply or block the Workflow objects.

2. Select the **Policy** tree from the Tree drop-down menu.
3. In the Policy tree, select the Policy where you want to block Workflow objects.
4. In the Blocked Workflows group box, click **Add**.
5. Select the Workflow object you want to block.
6. Click **Select**.
7. Click **Save/Apply**.

About Adaptable Workflows

Workflows are a powerful feature in Venafi Trust Protection Platform that allow you to wait for approvals, and to inject custom commands during remote key generation or provisioning.

Adaptable Workflows expand your ability to leverage workflows to meet several business needs:

- **External approvals.** If you already have an enterprise change management control system in place, you can use an adaptable workflow to integrate that third-party tool into the certificate workflow process.

For example, you could use the workflow to generate a change request in ServiceNow, and then take action on the certificate workflow depending on the result of the change request approval in ServiceNow.

- **Automatic approvals and rejections.** With an adaptable workflow, you can automatically approve or reject requests depending on the business needs and internal processes of your organization. Using this feature can dramatically improve the time it takes for certificates to be issued. With a manual certificate workflow, you might wait for hours or days for a human to manually review and approve every certificate request. When an Adaptable Workflow script has approval business logic built-in, the approvals matching those parameters can be approved in just a few seconds.

For example, you can automatically approve if the certificate is being renewed, or if the certificate is being renewed and nothing has changed between the current request and the previous version. You could also automatically reject the request if it includes an unsafe or unapproved keysize or algorithm.

- **Enhanced control over approvers.** Using scripts you can have greater control over approvers, doing things like ensuring a trusted group is always added to every approval, or ensuring a person cannot approve their own request, even if they are normally authorized to perform approvals.

DID YOU KNOW? 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 Workflow prerequisites](#)" below.

Take a look at our [sample implementation on Venafi's Cool Solutions](#).

Adaptable Workflow prerequisites

Before you configure a Adaptable Workflow application object in Trust Protection Platform, review the following prerequisites:

- Review the Adaptable Flow design to understand where you want the custom logic to be applied.
- 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.
- Install Windows PowerShell 3.0 or later.
- Install .NET 4.8 or later.

- Make sure you have a username credential that is valid for the device you will connect to. This is the username and password SSH Protect will use to connect to the device. For information on working with credentials, see [Creating user name or password credentials](#).
- Check out the sample script in the `\Venafi\Scripts\AdaptableSSHManagement\sample\` folder. This will help you create your script. Your scripts should be stored in the `\Venafi\Scripts\AdaptableSSHManagement\` folder. You will only be able to select items that appear in that specific folder, not any descendant folders.

What's Next

After you've completed the Adaptable Workflow prerequisites, see ["Creating an Adaptable Workflow" on page 588](#).

PowerShell script reference for Adaptable Workflow

Similar to other Venafi Adaptable solutions, the Adaptable Workflow utilizes a PowerShell script that contains functions you can use to integrate with third-party change management approval systems, or to perform automatic approvals and rejections of requests based on specific criteria.

TIP When creating new PowerShell scripts for use with the Adaptable Workflow (or other Venafi Adaptable solutions), keep in mind that the file name is used to identify your script from within the associated object in Trust Protection Platform. Using logical names can help you and other administrators recognize the purpose and intent of each script.

This section documents all available PowerShell functions for use with the Adaptable Workflow driver. PowerShell scripts are stored in the `\Venafi\Scripts\AdaptableWorkflow` 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 Workflow 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.

Sample scripts are provided in the `\Venafi\Scripts\AdaptableWorkflow\Samples` folder. Only files that are in the main `\Venafi\Scripts\AdaptableWorkflow\` folder can be selected in an Adaptable Workflow object in Policy Tree. Files in all sub-folders are ignored.

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 Workflow"](#) below.

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).

About debug logging

When a user has requested debug logging by checking **Enable Debug Logging** for Adaptable Workflow, 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 Workflow, see ["Creating an Adaptable Workflow"](#) on page 588.

About hash tables for Adaptable Workflow

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:

- Functions must not return errors; rather, they must throw exceptions in the same way that actual PowerShell errors do. The Adaptable Credential Adaptable SSH Key Discovery feature treats exceptions thrown by a PowerShell function as a fatal error and then halts processing.
- Thrown exceptions are handled as unexpected. If there is an error, we recommended you use `Result="Failure"` and pass the error description in the `Error=""` parameter.
- All functions (except where noted) must be present in the script, but they are optional from a logic standpoint.
- In the function references that follow, the following two functions are listed as not being required: `GetConfigPath`, and `CleanUP`. This means they are optional to implement. However, they should still be present in the script, and should return `Result="Success"` even with empty result data.

Creating new data fields for Adaptable Workflow

The Adaptable Workflow configuration provides a common set of variables you would typically need for processing workflows.. However, if you need to pass unique or additional data to your , you can define up to additional text fields. You do this by simply modifying the **Begin Field Definitions** section of the Adaptable Workflow PowerShell script.

PowerShell script field definitions

```

15 -----BEGIN FIELD DEFINITIONS-----
16 Text1|Minimum Key Size|10
17 Text2|Don't Allow Requestor to Approve|11
18 Text3|Text Field #3|00
19 Text4|Text Field #4|00
20 Text5|Text Field #5|00
21 Text6|Text Field #6|00
22 Text7|Text Field #7|00
23 Text8|Text Field #8|00
24 Text9|Text Field #9|00
25 Text10|Text Field #10|00
26 Text11|Text Field #11|00
27 Text12|Text Field #12|00
28 -----END FIELD DEFINITIONS-----
29

```

Adaptable Workflow object settings

Adaptable Workflow Settings

PowerShell Script: SouthAmericaWorkflow

Service Address:

Credential:

Secondary Credential:

Minimum Key Size: 1024

Don't Allow Requestor to Approve: ☒

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 Workflow 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 a mandatory field for capturing the minimum key size (so you can automatically reject certificates using a key size smaller than specified). Using a text (or PowerShell script) editor, you would open your PowerShell script file (which must be in the `drive:\Program Files\Venafi\Scripts\AdaptableWorkflow` folder). You would then edit the field definitions in the header section to include a new field labeled `<field name>` and set values for the available flags:

```
-----BEGIN FIELD DEFINITIONS-----
Text1|Minimum Key Size|11
Text2|Text2|00
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 Workflow 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 Workflow data fields

1. Open your Adaptable Workflow PowerShell file using a text (or PowerShell script) editor.
Adaptable Workflow PowerShell script files must be stored in the `\Venafi\Scripts\AdaptableWorkflow\` 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:
4. When you are finished, save the file and close it.

Your new field should appear on the Adaptable Workflow object page in Policy Tree.

Process function

With Adaptable Workflow, there is only one function supported in the PowerShell script. This function, called *Process*, is called every time Trust Protection Platform calls on the script. Use this function to send and receive data from an external system.

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.

Variable Name	Data Type	Description
OAuthAccessToken	String	OAuth token passed to the PowerShell script. Tokens are passed only after you've provided the required information in the <i>WebSDK OAuth Token Configuration</i> settings of the Adaptable object. See Configuring the Adaptable Log Channel object. 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.
ServiceAddress	String	The network address (e.g. URL) of the service with which the Adaptable Workflow interacts.
UserName	String	The user name portion of the user name credential assigned to the Adaptable Workflow instance. Used to authenticate with a remote system or service.
UserPass	String	The password portion of the user name credential assigned to the Adaptable Workflow instance. Used to authenticate with a remote system or service.

Variable name	Data Type	Description
WorkflowDN	String	Data representing the DN of the Adaptable Workflow object.
ObjectDN	String	Data representing the DN of the object being processed.
ObjectClassName	String	The class type of the 'ObjectDN' being processed.

Variable name	Data Type	Description
RequestedBy	String	The prefixed universal (universal name of an identity, prefixed by the name) of the user who initiated the workflow by clicking 'Renew' or 'Push' on the application.
CertificateVaultId	Integer	If the object type is a certificate, this parameter will contain the certificate VaultID. If the object type is not a certificate, this parameter is empty.
TppWebSdkUrl	String	String representing the fully-qualified domain name to the WebSDK of your Trust Protection Platform server. For information on where this variable data is set, see Trust Protection Platform server configuration.
WorkflowStage	Integer	The stage assigned to the Adaptable Workflow object.
WorkflowApprovers	Comma-separated string	List of identities allowed to approve the ticket.
WorkflowReason	String	The reason description assigned to the Adaptable Workflow object.
ReferenceId	String	The ID sent by the script to Trust Protection Platform, which Trust Protection Platform sends back in the subsequent go around. For example, this may be the ticket number in the external system. The ReferenceId is stored on the certificate or application object linked to the ticket. When the script is called again, "ReferenceId" will be passed back to the script.

Return	Data Type	Description
Result	String	One of the following results: ▪ Rejected. This is used when the script determines that processing should not continue. ▪ Approved. (Maps to WorkComplete state.) Used when the script approves the request without needing to create an internal ticket in Trust Protection Platform. ▪ Pause. (Maps to TicketIssued state.) Used to force the script to wait for a period of time before trying to process the request again. ▪ TicketRequested. Used when the script cannot approve or reject itself and needs to create a standard approval ticket in Trust Protection Platform for a human to review and approve.
Details	String	A field where you can provide additional information about the result being passed. This information is logged. Result types supported: ▪ All If the result type is <i>Rejected</i> or <i>Paused</i>, the information in the Details variable will show up in the user interface as the "Status" of the certificate or application.

Return	Data Type	Description
SecondsToPause	Integer	Length of time, in seconds, for the process to wait before attempting to run the workflow again. Result types supported: ■ Pause
WorkflowApprovers	Comma-separated string	A comma-separated list of prefixed universal identities that will be used as the approvers for the ticket that will be created in Trust Protection Platform. If no approver is passed in, the workflow driver uses the approvers specified in the workflow object. Result types supported: ■ TicketRequested
Referenceld	String	The ID sent by the script to Trust Protection Platform which Trust Protection Platform will send back in subsequent requests. The Referenceld is stored on the certificate or application object linked to the ticket. Result types supported: ■ Pause

Handling of unexpected script errors

When an unhandled error happens in an Adaptable Workflow PowerShell script, the error is caught by Trust Protection Platform, and is fully logged, to help you see the troubleshooting details.

Creating an Adaptable Workflow

Creating and configuring an Adaptable Workflow object is similar to creating any other workflow, except that you must specify the PowerShell script you want to use.

To create and configure a new Adaptable Workflow object

1. From the **TLS Protect** menu bar, click **Policy Tree**.
2. On the Policy tree, browse to the object that contains the certificates you want to process with the Adaptable Workflow.
3. Click **Add > Workflow > Adaptable Workflow**.
4. Enter the values on **Add New: Adaptable Workflow** page.

Section	Field	Description
General		
	Adaptable Workflow Name	Enter a name for this workflow configuration.
Adaptable Workflow Settings		
	PowerShell Script	Select the PowerShell script that you want to run with this workflow. You can only see scripts that are located in the <Venafi Home>\Scripts\AdaptableWorkflow\ folder, but not any of its subfolders.
	Service Address	Identifies the endpoint (URL, host, port, etc.) of the calling Adaptable Workflow object.
	Credential	Use to select the primary credential (username and password combination) to pass to the script. NOTE If you're connecting to the Venafi Web SDK, leave both credential files empty since you'll be specifying a credential in the WebSDK OAuth Token Configuration settings.
	Secondary Credential	Use to select a secondary credential to pass to the script, for example, to authenticate to the remote system.

Section	Field	Description
	Enable Debug Logging	(Optional) If you want to enhance troubleshooting capabilities of your Adaptable WorkflowAdaptable 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 581 in the Adaptable WorkflowAdaptable Flow PowerShell script reference.
Conditions		
	If Stage is	Applies the workflow actions at the designated stage of the object lifecycle. For more details on certificate workflow stage codes, see "Workflow object settings" on page 565.
Approvals		
	Request Approval From	Under the designated conditions, Trust Protection Platform submits an approval request to the workflow approver. You can request approvals for certificate renewals. The following options allow you to define the workflow approver. ◦ Approver assigned to object ◦ Specified approver ◦ Approver specified in PowerShell script

Section	Field	Description
		If you select either of the first two options, Trust Protection Platform will send the approvers list to the script. If you choose the third option, then you either don't need approvers, or the approvers are specified in the script or in the external system that you are connecting with.
	Specified Approvers	Defines a static approver for the workflow object. When selecting identities, press Ctrl+click to select multiple users and/or groups. If the Adaptable Workflow PowerShell script contains the "WorkflowApprovers" parameter, that value overrides the value set here on the workflow object, allowing the script to modify the approvers and pass back the updated list to Trust Protection Platform. If the script contains the WorkflowApprovers variable, that's what is used. If the script doesn't contain WorkflowApprovers, then Trust Protection Platform uses the approvers specified in the Trust Protection Platform interface.
	Approval Reason Code	Reason Code you want to include with the notification that is sent to the workflow approver. The maximum Approval Reason Code value is 999. NOTE This option is not required if you choose <i>Approvers specified in PowerShell</i> script. Otherwise it is required.

Section	Field	Description
		Approval Reason Codes also accompany customized explanations or instructions for workflow approvers. The drop-down list displays the Reason Codes defined in the Workflow tree. For more information, see "Defining reason codes for certificate approvals" on page 573.
WebSDK OAuth Token Configuration		
NOTE If your application doesn't connect to the Web SDK, leave all of these fields blank.		
	OAuth Token Application ID	Enter the application ID of the <i>API application integration</i> you should have created previously, as described in Adaptable Log Channel prerequisites .
	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. 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 you have specified custom fields in the PowerShell script, they will also be visible on this screen. Custom fields support macros that will be evaluated and the results will be passed to the PowerShell script. For example, the `$SelfDN$` macro will resolve to the DN of the certificate or application being processed for approval. For more information on Macros, see [Macro overview](#) in the *Macro Guide*. For more information on Configuration Macros, see [Configuration macros](#) in the *Macro Guide*.

Protecting against unapproved changes to Adaptable Workflow scripts

Venafi's Adaptable drivers—including Adaptable Workflow—rely on PowerShell scripts stored in the `\\Venafi\Scripts\AdaptableWorkflow` 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 Following an upgrade to Trust Protection Platform, you must take specific steps on all existing Adaptable Workflow objects in order for them to be re-enabled. That information is found in the following section.

When you encounter an error stating that the associated Adaptable Workflow PowerShell script has been modified, you'll need to open the Adaptable Workflow object where you assigned the script and re-save the object. When you do, the object is then re-enabled and you can continue using the script.

To re-enable an Adaptable Workflow driver following a change to its associated PowerShell script

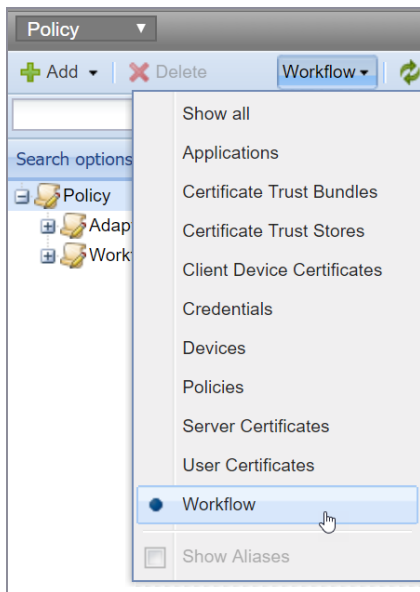
1. On the Venafi application server, open and review the associated scripts to verify that they contain only approved changes.
2. Open the Policy Tree and then open the Adaptable Workflow object where you assigned the associated PowerShell script.

3. On the Adaptable Workflow object, if you see an error message telling you that the PowerShell script needs approval, click **Save** at the bottom of the page.

Repeat these steps for all your Adaptable Workflow objects.

To locate all Workflow objects in your system

1. From the [Platform menu bar](#), click Policy tree.
2. On the **Show All** drop-down, select **Workflow**.



3. Expand the folders to see workflow objects.

Adaptable Workflow objects can be identified by the puzzle-piece icon overlaid on the workflow icon:



Managing approval requests in the Policy Tree

Approvers can manage their assigned Approval Requests in the Workflow tree in the Policy Tree. Approvers can see their own approved, pending, and rejected Approval Requests.

For information on how the standard way users can see their approval requests, see ["Managing certificate approval requests"](#) on page 596.

To immediately approve or reject a pending Approval Request using Policy Tree

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. Select the **Workflow** tree from the Tree drop-down menu.
3. In the Workflow tree, select **Pending**.
4. Select the Workflow Approvals you want to approve or reject.
5. Do one of the following:
 - Click  to approve the Approval Request.

If a Workflow Injection Command Request is approved, Trust Protection Platform executes the SSH stream command.

- Click  to reject the Approval Request.

If a Workflow Injection Command Request is rejected, Trust Protection Platform does not execute the SSH stream command.

To schedule an approval for later

Scheduling approvals is especially handy for Provisioning and Enrollment.

When you're ready to approve requests, you can schedule approvals for a later time and set the duration, or window, during which the approval can take place.

1. From the [TLS Protect menu bar](#), click Policy Tree.
2. Select **Workflow** from the drop-down menu.
3. In the Workflow tree, select **Pending**.
4. Select the Workflow Approval(s) you want to approve or reject.
5. Click  **Approve**.
6. Choose **Schedule Approval**.
7. Specify the date and time for the approval and then select **Approval Duration**.

For more information, see ["About approval duration" on page 599](#).

8. Add comments, as needed.

9. When you're done, click **Save**.
10. Click **Scheduled** to see your scheduled approvals.

To edit a scheduled approval

1. From the **TLS Protect menu bar**, click Policy Tree.
2. Select **Workflow** from the drop-down menu.
3. In the Workflow tree, select **Scheduled**.
4. Click the approval you want to edit. Details about the approval are displayed.
5. To change the schedule, click  **Approve**.
6. In the **Approval** window, select **Schedule Approval**.
7. Edit the approval details then click **Save**.

NOTE If you change the approver for an item that is pending approval, the update may take up to four hours to complete. Changing this setting can adversely affect performance of the system. If you need to change this setting contact Venafi Support.

To specify a ticket expiration period for an approval

1. From the **TLS Protect menu bar**, click Policy Tree.
2. Select **Workflow** from the drop-down menu.
3. Click the **Settings** tab.
4. In the Ticket Expiration box, enter the number of days a ticket can remain in Pending status before it is rejected.
5. When you're done, click **Save**.

Managing certificate approval requests

TLS Protect users can manage the approval requests that have been assigned to them. This involves reviewing the details of each request, making an informed decision, and then either approving or rejecting the request based on its merits.

Users with the Master Admin role can view and approve any request in the system. On the page displaying a user's approval requests, they are able to filter between their assigned approval requests and all approval requests in the system. See [Managing certificate approval requests](#).

NOTE Unlike the Policy Tree, TLS Protect's modern interface requires the approver to have both *View* and *Read* permissions to the certificate, and/or the installation that is being reviewed and approved. Be sure to set the permissions before you continue.

For information about how users can see their approval requests in the Policy Tree, see "[Managing approval requests in the Policy Tree](#)" on page 594.

To approve or reject a pending Approval Request

1. Log in to the TLS Protect product, and browse to the **All Certificates (dashboard)**.

TIP You can also open the Certificate list, and use the **Pending My Approval** quick filter, then skip the next step.

2. In the Certificate Totals widget, locate the **Pending My Approval** section.

If there are items you can approve, the **Pending My Approval** section will have a number greater than 0. Click the number to view those certificates that are pending your approval.

NOTE If there are no items you can approve, the **Pending My approval** section will show 0.

When you click the number, you are taken to the Certificate list, with a filter applied that shows you items needing your approval.

3. The certificate list shows either certificates that need your approval, or certificates that have a pending installation that needs your approval.
 - If the certificate itself needs approval, you can use the quick action to either approve or reject the certificate.
 - If the certificate has an installation that needs approval, you won't see a quick action to approve or reject the certificate. Instead, click the down arrow next to the installations field to see the certificate installations. If there are more than one installations, the item(s) that require approval show **Approve/Reject** on the quick action button.
4. Click the **Approve/Reject** button.
5. In the modal window, review the request. If the request is for a certificate installation, then determine if you want to Approve Now (default), or Schedule Approval. (Scheduled approvals are only available for certificate installations.)

- [Optional] In the **Comments** field, enter your reason for rejecting or approving this request. Especially if you are rejecting the request, this information will help the requester know what needs to be changed or why the request was rejected.
- To approve now, select the **Approve Now** option at the top of the form, and then click **Approve**.
- To schedule the approval to happen at a later time, select the **Schedule Approval** option at the top of the form, and then click **Approve**.

The scheduling option appears. Enter the date and time (in your current time zone) when you want the approval to occur, then select the approval duration (in hours).

For more information on approval duration, see ["About approval duration" on the facing page](#)

6. Click **Approve** or **Reject**.

To edit a scheduled approval

1. From the [TLS Protect menu bar](#), click **Inventory > Certificates**.
2. In the **Common Filters > Status** field, filter on **Approval Scheduled**.

If there are scheduled items you can edit, they will be displayed in the certificate list.

3. The certificate list shows either certificates that have been scheduled for approval, or certificates that have a pending installation that is scheduled for approval.
 - If the certificate itself is scheduled for approval, you can use the quick action to Edit the approval.
 - If the certificate isn't scheduled for approval, but has an installation whose approval is scheduled, you won't see a quick action to Edit the Approval for the certificate. Instead, click the down arrow next to the installations field to see the certificate installations. If there are more than one installations, the item(s) that are scheduled for approval show **Edit Approval** on the quick action button.
4. Click the **Edit Approval** button.
5. In the modal window, you can change the approval to **Approve Now**, or you can modify the schedule for the approval.
 - To approve now, select the **Approve Now** option at the top of the form, and then click **Approve**.
 - To modify the approval schedule, modify the date and time (in your current time zone) when

you want the approval to occur, then select the Approval duration (in hours).

For more information on approval duration, see ["About approval duration" below](#).

NOTE If you change the approver for an item that is pending approval, the update may take up to four hours to complete. Changing this setting can adversely affect performance of the system. If you need to change this setting contact Venafi Support.

6. Click **Approve** or **Reject**.

About approval duration

If you choose to schedule an approval for a workflow approval request, you can specify a window of time during which the approval can take place. This is called the *Approval Duration*.

To learn more about scheduling an approval, see ["Managing approval requests in the Policy Tree" on page 594](#).

Approval Duration in Policy Tree

How it works

- When you set the Date/Time for approval, the Trust Protection Platform processes all scheduled approvals at that time. If for some reason the approval process cannot be completed at the scheduled time, e.g., the Venafi Server or Venafi Database is down, then Trust Protection Platform will run approvals as soon as the Venafi Server or Venafi Database is running again.
- When you select Approval Duration, you specify a window of time during which approvals can take place after the process is started. Approval Duration allows you to control when the approval process will run. If you don't set a duration (Policy Tree only), then, if the initial approval time is missed, the approval process will begin as soon as the server or network is running again. If you set a duration and the window is missed, you must reschedule approvals.

EXAMPLE Suppose approvals are scheduled for 1:00 a.m. on November 7, 2024. However, the Venafi Database goes down at 12:45 a.m. that day due to an unscheduled maintenance event. If Venafi Platform comes back up before 3 a.m. (inside the 2 hour window) then the approval process begins. If Venafi Platform comes up after 3 a.m. (outside the 2 hour window), then you must reschedule approvals.

Approval Duration allows you to specify a window of time during which approvals can take place if the initial approval time is missed.

About Date/Time

The time zone displayed is the OS clock time and is localized.

EXAMPLE Suppose the administrator viewing Approvals is in Denver, Colorado. The Date/Time is displayed as *Mountain Daylight Time*, 11/07/2024, and 1:00:00 AM. When another administrator in New York views Approvals, the time zone changes to Eastern Daylight Time. The Date/Time is displayed as *Eastern Daylight Time*, 11/07/2024, and 3:00:00 AM.

CAUTION Scheduling approvals without specifying an Approval Duration. If for some reason the approval process cannot be completed at the scheduled time, e.g., Venafi Server or Venafi Database is down, then Trust Protection Platform will run approvals as soon as the Venafi Server or Venafi database is running again. This could interfere with other network processes.

Approval Duration in Aperture

NOTE In Aperture, **Approval Duration** is a required field.

How it works

- When you set the Date/Time for approval, the Trust Protection Platform processes all scheduled approvals at that time. If for some reason the approval process cannot be completed at the scheduled time, e.g., the Venafi Server or Venafi Database is down, then Trust Protection Platform will run approvals as soon as the Venafi Server or Venafi Database is running again.
- When you select Approval Duration, you specify a window of time during which approvals can take place after the process is started. Approval Duration allows you to control when the approval process will run. If you don't set a duration (Policy Tree only), then, if the initial approval time is missed, the approval process will begin as soon as the server or network is running again. If you set a duration and the window is missed, you must reschedule approvals.

EXAMPLE Suppose approvals are scheduled for 1:00 a.m. on November 7, 2024. However, the Venafi Database goes down at 12:45 a.m. that day due to an unscheduled maintenance event. If Venafi Platform comes back up before 3 a.m. (inside the 2 hour window) then the approval process begins. If Venafi Platform comes up after 3 a.m. (outside the 2 hour window), then you must reschedule approvals.

Approval Duration allows you to specify a window of time during which approvals can take place if the initial approval time is missed.

About Date/Time

The time zone displayed is the OS clock time and is localized.

EXAMPLE Suppose the administrator viewing Approvals is in Denver, Colorado. The Date/Time is displayed as *Mountain Daylight Time*, 11/07/2024, and 1:00:00 AM.

When another administrator in New York views Approvals, the time zone changes to Eastern Daylight Time. The Date/Time is displayed as *Eastern Daylight Time*, 11/07/2024, and 3:00:00 AM.

CAUTION When you set the Approval Duration, you specify a window of time during which approvals can take place after the process is started. Approval Duration allows you to control when the approval process will run. If you set a duration and the window is missed, you must reschedule approvals.

About workflow approvers

When a certificate is created, approvers are assigned to the certificate. This may be an individual, several individuals, a group, or a combination of these.

When a workflow is created, its creator can choose to use the default approvers on the certificate, or override the default approvers either with a specific list, or with a script. If an approver is set by the workflow, and it is different than the approvers on the certificate, the approvers set on the workflow override the approvers set on the certificate.

In the certificate inventory, you can add the column "Approvers" to see the approvers set on the certificate. However, this may not be the actual list of approvers, if a workflow operation overrides the default approvers.

If a workflow is in a state of pending approval, you can open the certificate details page, and in the Pending Approval banner at the top, click "See Approvers" to see which approvers the certificate is waiting on. The list will show the approvers, regardless of whether they are the default approvers, or whether the list comes from the workflow.

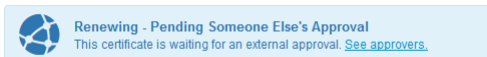
Viewing pending approvers for a workflow

If a workflow is pending approval, you can see a list of approvers, at least one of which must approve the workflow before the requested process can continue.

NOTE You must have *View* and *Read* permissions to a certificate or an installation to see who a blocking approval workflow is waiting for.

To view the list of pending approvers on a certificate

1. From the **TLS Protect menu bar**, click **Inventory > Certificates**.
2. In the **Common Filters** section, in the **Status** field, add the following status: **Pending Someone Else's Approval**
3. Locate the certificate whose approvers you want to see, and click the certificate's nickname.
4. In the **Renewing - Pending Someone Else's Approval** banner, click **See approvers**.



A modal window lists the identities from whom the certificate is pending approval.

5. Click **Close** to continue.

#

403 488

403 admin 488

403 aperture 488

403 error 488

403 forbidden 488

A

abort

discovery jobs 110

account settings

Aperture 437

ACME 251

certbot 252, 258

certbot commands 259

change engine hostname 256

domain challenge 257

in Aperture 254

installing 254

integration with Trust Protection
Platform 251

request certificate 258

viewing certificates 262

Adaptable

configuring onboard discovery 73, 84

Onboard Discovery sample script 80

Adaptable Bulk Provisioning

PowerShell script reference 520

protecting against unapproved script
changes 524

Adaptable CA

Certificate Import

about updating PowerShell scripts when
service URL or configuration
changes are made 126

setting up certificate import 123

Adaptable Workflow

PowerShell script reference 580

protecting against unapproved changes 593

agentless provisioning 500

agents

search filter

how it works 403

searching for 400

using for certificate installation 508

algorithms

key 443, 446

Amazon Web Services

configuring onboard discovery for 73, 84

Aperture

Discovery page 103

folder 177

Jobs 103

policy permission 177

searching and filtering for objects in 400

appliances

importing certificates and configurations
from 70

application object

associating with a certificate 203, 206

application object configuration

via Aperture 509

application objects

managing 509

applications

associating to certificates 202

managing 509

pushing, certificate and private key to 249

apply filters 37

approval

certificate installation 512

edit scheduled 596, 598

specify ticket expiration 596

approval scheduled 39

approved CAs 198, 326

Approver 601-602

automatic renewal 489

awaiting CSR 39

Azure

configuring onboard discovery for 73, 84

B

backoff 451

blacklisting

root or intermediate root certificates 338

BlueCoat

trust store configuration 352

bulk move

certificates 112, 472

Bulk Provisioning

about 514

Adaptable PowerShell sample script 518

Bulk Provisioning Manager service module
settings 528

creating a new job 515

editing an existing job 525

Imperva MX sample PowerShell script 518

jobs

running manually 109

prerequisites 515

renaming a job 526

running a job manually 527

scheduling a job 525

service module settings 528

Symantec SSL Visibility Appliance sample
powershell script 518

viewing log events 529

viewing logs 528

C

ca compromise 230

CA import

enabling or disabling 131

- running import job manually 128
- CA imports
 - manually running import job 128
 - reconciliation rules 129
- CA Templates
 - creating self-signed template object 296
- CAPIC
 - configuring onboard discovery 73, 84
 - trust store, configuring 354
- CDP 228
- cdp 241
- CDP monitoring
 - disabling 235
 - enabling 235
- CDP status 241
- CDP verification 241
- certbot 251
- certificate 185, 311, 476
 - associating with applicaiton objects 203, 206
 - creating 440
 - deleting 471
 - get new 440
 - importing existing 135
 - resolving errors 469
- Certificate and Device Placement 98
- certificate and device placement
 - jobs
 - running manually 109
- certificate approval 451, 484, 594, 596
- certificate approval delay 451
- certificate authorities 451
- certificate creation 451
- certificate details 185, 311
- certificate enrollment
 - SCEP 265
- certificate expiration
 - tracking 437
- certificate hold 230
- certificate import 135
 - creating a Microsoft CA import job 120

- creating an Adaptable CA import job 123
- from an Amazon Private CA 118
- jobs
 - creating 118, 120, 123
 - running manually 109
- reconciliation rules 129
- Certificate Import
 - Adaptable CA
 - about updating PowerShell scripts when
 - service URL or configuration
 - changes are made 126
- certificate in error 38
- certificate installation 475-476, 479, 482, 484-485
 - agentless 496
 - approving or rejecting 512
 - approving workflows 513
 - configuring devices for 498
 - editing 483
 - how it works 493
 - see provisioning 496
 - statuses explained 531
 - using the Server Agent 508
 - viewing in a report 411
 - with or without the Server Agent 496
- certificate inventory 37
- certificate inventory list 37
 - columns 411
 - sorting and reordering columns 411
- certificate issuance backoff 451
- certificate issuance delay 451
- certificate issued 40
- certificate lifecycle 23, 489
 - stages 27
- certificate managed 40
- certificate management 479
- certificate management types
 - levels of 154
- certificate objects
 - configuring 145, 302
- certificate placement 98, 111

- certificate renewal 489
- certificate revocation 223, 227, 236, 463
 - about reason codes 230
 - CRL overview 236
 - disabling monitoring 235
 - enabling 235
 - viewing status of multiple certificates 236
- certificate revocation lists
 - see CRL 247
- certificate risk 37
 - disabled validation 42
 - distrusted Symantec 40
 - failed validation 40
 - invalid domain name 41
 - local dual control needed 41
 - lost 41
 - no owner assigned 41
 - no provisioning targets 41
 - unapproved issuer 42
 - unique name violation 42
 - unsafe validity period 42
 - weak key 43
 - weak signing algorithm 43
 - wildcard prohibited 43
- certificate risks 37
- certificate status 37
 - approval scheduled 39
 - awaiting CSR 39
 - disabled 38
 - expired-long term 39
 - expired-short term 39
 - expiring soon 40
 - failed revocation 38
 - in error 38
 - installing 39
 - issued 40
 - managed 40
 - management type unassigned 38
 - not disabled 40
 - pending my approval 38

- pending revocation 39
 - pending someone else's approval 39
 - renewing 39
 - revoked 39
- Certificate Summary 185, 311
- certificate workflow 451, 484
- certificates
 - about managing certificates 439
 - about managing network certificates 133
 - about workflow management 557
 - approved issuer 190, 319
 - associating to applications 202
 - automated discovery 55
 - bulk move 112, 473
 - configuration
 - managing 139
 - creating 447
 - CRL verification 241
 - download 453
 - downloading PEM with contents extracted
 - into .crt and .key files 457
 - extracting 213
 - filtering and searching 400
 - finding a specific user's 409
 - importing from appliances 70
 - importing using Onboard Discovery 70
 - install using Bulk Provisioning 514
 - install using the Server Agent 508
 - lifecycle management 27
 - lifecycle stages 28
 - local object settings 303
 - lost 399, 417
 - manage via policy 317
 - management type 27, 190, 319
 - management types 22, 154
 - managing 19
 - overview 21
 - managing on local file systems and
 - keystores 293

- network
 - managing 135
- pushing 249
- reactivating after retiring 466
- renaming 470
- renewing 214, 447, 461, 529
- retiring 447, 465
- retrieving 137
- revoking 223, 447, 463
- revoking manually 220
- schedule renewal 468
- search filter
 - how it works 403
- taking ownership 418
- unassigned 146, 155, 179
- view details 448

Certificates 37

chain building

- blacklisting root certificates 338

- change of affiliation 230

configuration object

- Aperture 419

Connect

- Direct

- configuring trust store 359

- credentials 481

CRL

- enabling verification checking 241

- notifications 248

- overview 236, 238

- setting expiry notification percentage 247

CRL Distribution Point 241

- Status 241

CRL Verification 241

D

DataPower

- configuring trust store 356

- delete certificate installation 479

deleting

- jobs defined in Aperture 108

- device
 - change the provisioning mode 500
 - settings for 500
- device credential
 - setting or editing 499
- device objects
 - using with Bulk Provisioning 515
- disable certificates 465
- disabled certificate 38
- disabled certificate status 38
- discovery 62, 111
 - canceling manually 110
 - editing jobs 106
 - editing the order of placement rule execution 93
 - excluding specific host names during 63
 - excluding specific IP addresses during 63
 - filtering the Jobs list by job type 104
 - Jobs list in Aperture 103
 - managing jobs 103
 - managing your discovery server 61
 - methods for discovering certificates and keys 55
 - methods for discovering certificates and keys 55
 - packets 55
 - pausing manually 110
 - permissions required for discovery on appliances 70
 - prioritizing jobs 106
 - renaming a job 107
 - running job manually 109
 - running manually 110
 - running manually in Policy Tree 83
 - scheduling a discovery job 105
 - specifying exclusion objects 115
 - using Bulk Provisioning 55
 - using Network Discovery 55
 - using Onboard Discovery 55
 - using Server Agents 55

discovery module

managing 61

Discovery Zones 62

distrusted Symantec 40

domain components 441, 491-492

drivers

configuring self-signed certificate CA
template object 296

duplicate certificates 111

E

ECC

key algorithm 446

see Elliptic Curve Cryptography 440

effective bundle

viewing 346

Elliptic Curve Cryptography (ECC) 440

Elliptical Curve Cryptography 446

enabling CDP monitoring 235

enabling certificate revocation 235

enabling certificate revocation monitoring 235

encryption

password-based 329

enforce host key 500

enrollment

certificate management type 154

exclusion objects

specifying for discovery 115

using to exclude addresses during
discovery 63

existing certificate 135

importing 135

expired long term 39

expired short term 39

expiring soon 40

expiry notification

setting for CRLs 247

extracting, certificate and private key 213

F

F5 Discovery

F5 Networks required version 73

F5 LTM

required Trust Protection Platform
permissions 73

F5 LTM Advanced

configuring onboard discovery 73, 84

F5 Networks

Onboard Discovery requirements 73

failed revocation 38

failed validation 40

FAQ

self-signed certificates 299

File Result 534-535, 549-550

file validation 533

agentless 535

using Server Agent 536

File validation 534-535, 548-550

File/Installation validation 534-535, 549-550

filtering 37

Discovery jobs list by job type 104

filters 37

using to find objects in Aperture 400

folder

permissions required to view 177

setting policy on 177

G

GeoTrust 40

GSK

trust store, configuring 364

H

historical certificates 187, 313, 489

downloading 316

reverting 315

revoking 314

host key 500

I

iControl REST API

used with Onboard Discovery 73

identities

 setting up 420

Imperva MX

 Sample PowerShell script for Adaptable
 Bulk Provisioning 518

implicit placement 111

importing

 certificates using Certificate Import 55

importing certificates 128, 135

 jobs

 creating 118, 120, 123

in error 38

Installation

 certificate

 how it works 493

 management 479

installation

 cancelling 484

 certificate (TrustForce) 531

installation type 475

 editing 482

installation validation 533

 agentless 535

 using Server Agent 536

Installation validation 534-535, 548-550

installing (certificate status) 39

Instant Discovery

 about 83

intermediate root certificate

 deleting 336

 importing 334

inventory 37

Inventory 37

inventory list 37

J

JKS

 trust store, configuring 367

job details 98

job type

 filtering Discovery jobs list 104

jobs 98, 108

deleting 108

renaming a bulk provisioning job 526

running bulk provisioning jobs manually 527

running manually 109

Jobs

editing a bulk provisioning job 525

Jobs list 103

jobs;prioritizing 106

jobs;prioritizing discovery jobs 106

K

key compromise 230

keys

about managing private keys 133

automated discovery 55

extracting 213

managing 19

pushing to applications 249

search filter

how it works 403

L

lifecycle stages

certificates 27-28, 565

local dual control needed 41

Log events

related to bulk provisioning 529

Log Server

notification rules 432

long term expired 39

lost certificate 41, 399, 417

M

managed 40

management type 38

management type unassigned 38

management types 146

editing 44, 511

managing application objects 509

Managing jobs 103

Microsoft Azure

configuring onboard discovery for 73, 84

Microsoft CA

setting up certificate import 118, 120

Monitoring

certificate management type 154

move certificates 87

N

NDE

see network device enrollment 265

network device enrollment

example rule execution 286

managing 265

setting rules for 283

settings for 277

Network Device Enrollment Settings tab 277

network devices

onboard discovery 73, 84

Network Discovery 111

deleting placement rules 94

editing jobs 106

jobs

Creating 58

running manually 109

scheduling 105

Move Certificates 112, 473

Placement Rules

Editing 90

prioritizing jobs 106

no owner assigned 41

no provisioning targets 41

not disabled certificate status 40

notification rules 432

notifications

about 428

customizing email 432

O

objects

- search filter

- how it works 403

OCSP 228, 236

Onboard Discovery

- about 70

- Amazon Web Services 73, 84

- CAPI 73, 84

- Citrix NetScaler 73, 84

- editing jobs 106

- F5 discovery requirements 73

- F5 LTM Advanced 73, 84

- IBM DataPower 73, 84

- jobs

- running manually 109

- scheduling 105

- Microsoft Azure 73, 84

- prioritizing jobs 106

- sample Adaptable PowerShell script 80

onboard discovery

- configure devices with Device credential 70

- configuring 73, 84

- jobs

- running manually 109

- permission requirements 70

- prerequisites 70

onboard validation 533-535, 549-550

- agentless 535

- using Server Agent 536

P

PBE 329

PEM

- extract and download PEM contents as
separate files 457

pending approval 38-39, 601-602

pending my approval 38

pending someone else's approval 39, 601-602

permissions

administrator 427

assign to Identities 422

associate 426

create 425

delete 425

manage policies 425

Onboard Discovery 70, 73

private key read 427

private key write 427

read 423

rename 426

required by Bulk Provisioning 515

revoke 427

view 423

write 423

PKCS#12 453, 456

configuring trust store 374

option missing 453

place certificates 87

place devices 87

place keys 87

placement 98

using Certificate and Device Placement 55

placement engine 87, 111

enabling 115

placement job

results 98

scheduling 98

placement jobs 98

placement rules 98, 111

deleting network discovery 94

editing the order in which they run 93

platform object

network device enrollment 277

policies

managing certificates 317

permissions required for folder 177

setting on a folder 177

settings for certificates 190, 319

policy object

- certificate settings 190, 319

PowerShell

- script reference for Adaptable Bulk Provisioning 520

PowerShell script

- reference for Adaptable Workflow 580
- sample script 127
- unapproved changes to 524, 593

PowerShell scripts

- sample scripts for Adaptable Bulk Provisioning 518

presented fingerprint 500

presented thumbprint 500

PRIME256 446

PRIME256v 446

PRIME256v1 446

prioritizing 108

private keys

- downloading 453

managing

- overview 21

password-based encryption 329

provisioning

- about 26
- choosing agent or agentless 496
- see Certificate Installation 513

Provisioning

- certificate management type 154
- certificates and key in bulk 515
- certificates and keys in large numbers 514

provisioning mode

- agentless 500
- set on device 500

Q

Quick Search

- using to find objects in Aperture 400

R

RapidSSL 40

reason codes 573

- certificate revocation 230

reconciliation rules

- CA imports 129

remove certificates 465

renaming

- bulk provisioning jobs 526

- Discovery jobs 107

renew certificate 214, 461, 489, 529

renewing (certificat status) 39

renewing certificate status 39

replace certificates 485

reports

- creating custom 411

retiring certificates 465

revocation 226-228, 236

- checking the status 228

- manually revoking certificates 220

- viewing status of multiple certificates 236

Revocation Check Now 226, 228

Revocation Check Status 228

Revocation Checking 226-228

revocation checking

- OCSP 228

revocation status 236

revoked 39

revoked certificate status 39

risk 37

risks, certificate

- explained 37

root certificate

- blacklisting from chain building 338

- importing 334

root chain

- downloading 453

root verification 241

RSA

- key algorithm 446

Run Now

- manually running a discovery job 110

S

SANS

- about 174

SCEP 265

scheduling 98

- bulk provisioning jobs 525

- certificate renewal 468

- trust store updates 389

- searching for objects in Aperture 400

SECP 446

SECP256 446

SECP256k 446

SECP256k1 446

self-signed certificates

- frequently asked questions 299

Server Agent

- provision certificates using 496

Server Name Indication

- validation 545

- short term expired 39

SNI

- validation 545

- sorting and reordering certificate inventory list

- columns 411

- SSH fingerprint 500

- SSH thumbprint 500

- SSL validation 534-535, 548-549

- SSL/TLS Validation 534-535, 549

- status 37

- status, certificate

- explained 37

- superseded 230

- Symantec 40

Symantec Managed PKI Service

- sample script for use with Adaptable CA driver 127

Symantec SSL Visibility Appliance

Sample PowerShell script for Adaptable
Bulk Provisioning 518

T

Thawte 40

TLS validation 534-535, 548-549

transaction ID 489

troubleshooting

Aperture 487

log events for bulk provisioning 529

trust assets

searching and filtering for 400

trust store

configure PKCS#12 374

using CAPI 354

using Connect

Direct 359

using DataPower 356

Trust Store Management 348

trust stores

JKS 367

managing 348

view effective bundle 346

TrustForce 493

U

unapproved issuer 42

Unassigned

certificate management type 154

unassigned certificates

about 27

unique name violation 42

unsafe validity period 42

user credential 481

V

validate Now 534-535, 548-550

validation 534-535, 548-550

configuring 544

application 546

- certificates 460, 545
- disabling 554
- disabling onboard 538
- disabling SSL/TLS 554
- overview 541
- running scans 486, 547
- SNI (Server Name Indication) 545
- supported certificate ciphers 545
- viewing results 548
- validation status 548
- Venafi Configuration Console
 - enabling or disabling CA Import 131
- Verify Now 241

W

- weak signing algorithm 43
- whitelisting
 - CAPI trust store configuration 354
 - certificates 339

- Connect
 - Direct trust store configuration 359
 - DataPower trust store configuration 356
 - domains 391
 - wildcard prohibited 43
 - win-acme 251
 - workflow 484, 601-602
- Approval
 - Scheduling 595
- Approval Duration
 - Time Zone 599-601
- implementing 557
- settings 565
- workflows
 - about 558

