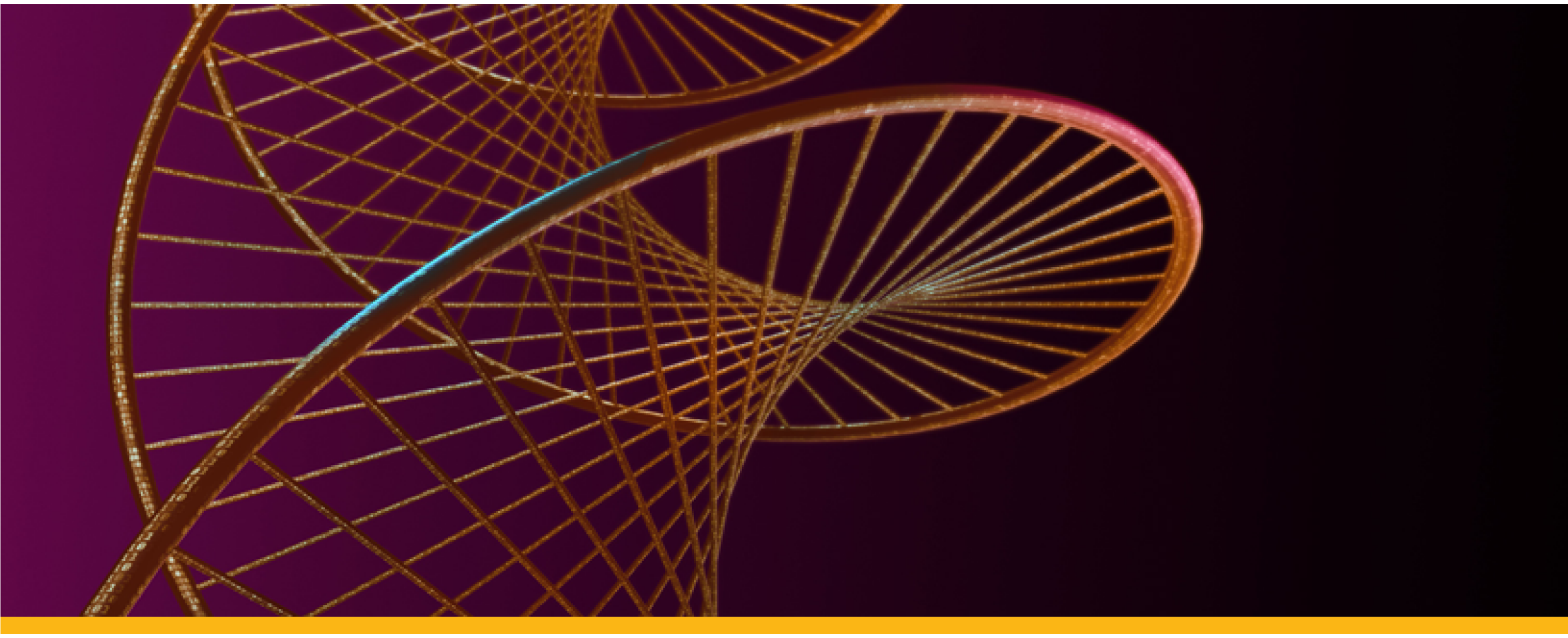
Venafi Trust Protection Platform 25.1

Overview Guide



Venafi
A CyberArk Company

Legal Notices

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 (Overview 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

About This Guide

Venafi™ protects machine identities for the largest companies on the planet. Leaders in the Global 5000 rely on Venafi to secure the cryptographic keys and digital certificates that authorize and control all machine-to-machine connections and communications.

Venafi delivers the only enterprise-class solution that automates the provisioning, discovery, monitoring, validation and management of digital certificates and encryption keys—from the desktop to the data center—built specifically for encryption management interoperability across heterogeneous environments.

Trust Protection Platform's architecture supports many certificate authorities (CAs), assorted platform deployments and various encryption types, and has proven scalability within the world's largest enterprises.

This *Product Overview Guide* provides a conceptual overview of Trust Protection Platform, including its system architecture, components, and administrative tools.

Audience

Venafi Trust Protection Platform documentation is written for administrators who are responsible for managing encryption assets and technologies across server-side systems and appliances using Venafi Trust Protection Platform.

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

Overview

Welcome to Venafi Trust Protection Platform™. Venafi Trust Protection Platform is an enterprise key and certificate management solution that helps you **secure and protect** your encryption assets across diverse operating systems and infrastructure environments–from the desktop to the data center. Within these environments, Venafi Trust Protection Platform centralizes the management of authentication and encryption technologies across server-side platforms, desktops, laptops, applications, and appliances where vital data resides and is transmitted.

With a robust set of tools typically associated with high-end IT management systems, administrators can now deploy, monitor, and enforce their organization's security and encryption folders with greater efficiency (and efficacy) than ever before.

This guide introduces you to the latest features in Venafi Trust Protection Platform and introduces the documentation resources provided to help you deploy, configure, and manage Venafi Trust Protection Platform.

Venafi TrustAuthority

Venafi TrustAuthority helps you protect your machine identities with continuous discovery and monitoring.

Once installed, Trust Authority™ gives you the global visibility and intelligence you need to determine which machine identities should be trusted, and fix or block those that should not. Discover and protect all keys and certificates that act as machine identities across your internal and external infrastructures: the internet and virtual, cloud and IoT.

Trust Authority™ gives you visibility and intelligence into your organization's certificate inventory:

Visibility: Locating all your certificates to learn where they're installed

- Create an accurate inventory of all TLS certificates
- Scan local systems to retrieve internal certificates
- Automatically connect to any CA to import certificates

Compliance: Creating strong certificates that comply with security policies

- Enforce enterprise-wide key and certificate security policies
- Structure policies based on flexible attributes
- Integrate with third-party workflow systems

Scalability: Scaling enrollment to support all business units

- Quickly issue new certificates
- Automate provisioning within popular DevOps frameworks
- Automate certificate requests and renewals

Proactive: Continuously monitoring all certificates for security and availability

- Schedule regular scans to detect anomalous use
- Coordinate alerts for impending certificate expirations
- Automate notifications of rogue keys or certificates

- Validate proper certificate installation and configuration

Venafi TrustForce

Once installed, Trust Force™ helps you to accelerate and scale protection with automated remediation and verification.

Automating machine identity protection helps to ensure the security and protection of your key and certificate inventories by orchestrating rapid, corrective actions at machine speed and scale.

Trust Authority™ gives you the automation to scale your encryption:

Automation: Orchestrating your PKI infrastructure

- Automate the replacement of expiring certificates to eliminate outages
- Manage certificate life cycles across multiple certificate authorities
- Automatically find, revoke and validate compromised certificates
- Orchestrate provisioning for encryption-dependent applications

Remediation: Automate remediation and verification at machine speed

- Quickly respond to a CA compromise or inadvertent error
- Seamlessly change, remove, replace or consolidate certificate authorities
- Verify that all remediation actions comply with security policies

Policy: Enforce governance to streamline compliance

- Define automated workflows, provisioning and change management controls
- Apply pre-defined security policies for continual validation
- Calibrate rule-based access controls to allow or block access
- Authenticate only policy-compliant machine identities

2

What’s New in 25.1

Venafi Trust Protection Platform™ version 25.1 introduces a number of powerful new features to help you solve your most important business problems related to securing and protecting keys and certificates within your organization.

To read about the new features, visit What's new in Trust Protection Platform's latest version.

To read about important considerations before upgrading to 25.1, visit Important considerations before upgrading.

3

About cloud integrations with Venafi

As business workloads have moved to the cloud, the need to secure and protect certificates and keys is greater than ever. Venafi is leading the way in securing and protecting digital assets in the cloud.

Cloud applications are most often designed for DevOps, which means that they are deployed and re-deployed frequently. This strategy has led to the use of more, shorter-validity certificates and all but eliminated concerns about problems caused by certificate expiration. Lifecycle automation is still important for user-facing certificates because if they're not renewed before they expire, they will cause outages.

Venafi integrates with Amazon Web Services and Microsoft Azure.

Amazon Web Services

- **Amazon Certificate Manager (ACM):** Amazon's certificate authority and primary certificate store

  Trust Protection Platform can facilitate the enrollment of certificates from the Amazon CA or upload certificates by other CAs to ACM, and then provision them to supported cloud services.

  See Amazon Amazon Certificate Manager–CA template configuration for more information.

- **Amazon Elastic Load Balancer:** Amazon's very popular solution for distributing network traffic across multiple application servers

Trust Protection Platform can automate the full certificate lifecycle by provisioning certificates issued by any CA to either application load balancer (ALB) or classic load balancer (ELB) listeners.

See Amazon Web Services (AWS)–Overview for more information.

- **Amazon CloudFront:** Amazon's content delivery network (CDN)

  Trust Protection Platform can automate the full certificate lifecycle by provisioning certificates issued by any CA to existing CloudFront instances.

  See Amazon Web Services (AWS)–Overview for more information.

- **Amazon Elastic Cloud Computing (EC2) Instances:** Virtual machines in the Amazon Web Services cloud

  These instances generally run the same Linux and Windows operating systems that Trust Protection Platform has supported using both agent and agentless provisioning inside the firewall. However, unlike traditional on-premise machines, EC2 instances usually have a much shorter lifespan. This is because they are expected to be created and destroyed as the load on the application increases and decreases. This difference is significant because a software configuration management solution is usually involved in the deployment of applications to new instances at the time of their creation; and that kind of solution is perfectly positioned to orchestrate the provisioning of a new certificate and private key to the instance.

Microsoft Azure

Azure Key Vault is Azure’s central secure repository for certificates, keys, and other secrets consumed by cloud applications. Trust Protection Platform can automate the full certificate lifecycle by provisioning certificates issued by any CA into an Azure Key Vault. Consumers of Azure Key Vault certificates and keys like Azure Web App Services are designed to automatically self-update whenever a new version of a certificate they’re using is provisioned to the Key Vault. This means that Trust Protection Platform doesn’t need to worry about what is using the certificate.

See Microsoft Azure and Trust Protection Platform integration for more information.

Venafi's open source projects on GitHub

Venafi sponsors more than fifteen GitHub repositories, open source projects that you can implement into your environment, or even improve and submit pull requests to. Some of Venafi's open source projects include:

- **vCert**. Go client SDK and command-line utility designed to simplify integrations by automating key generation and certificate enrollment using Venafi machine identity services.
- **valut-pki-monitor-venafi**. Venafi PKI Monitoring Secrets Engine for HashiCorp Vault that enforces security policy and provides certificate visibility to the enterprise.
- **vault-pki-backend-venafi**. Venafi PKI Secrets Engine plugin for HashiCorp Vault that enables certificate enrollment using Venafi machine identity services.
- **vCert-java**. Java client SDK designed to simplify integrations by automating key generation and certificate enrollment using Venafi machine identity services.
- **openstack-heat-plugin-venafi**. OpenStack Heat plugin that uses Venafi to streamline machine identity (certificate and key) acquisition.
- **vCert-python**. Python client SDK designed to simplify integrations by automating key generation and certificate enrollment using Venafimachine identity services.
- **vCert-ruby**. Ruby client SDK designed to simplify integrations by automating key generation and certificate enrollment using Venafi machine identity services.
- **terraform-provider-venafi**. HashiCorp Terraform provider that uses Venafi to streamline machine identity (certificate and key) acquisition.
- **ansible-role-venafi**. Ansible Role that uses Venafi to streamline machine identity (certificate and key) acquisition.
- **aws-private-ca-policy-venafi**. Venafi Lambda functions for AWS that enforce enterprise security policy for the AWS Private CA.

To learn more about these (and other) Venafi open source projects, visit our GitHub page at https://github.com/Venafi.

4

System Management

Venafi Trust Protection Platform™ automates the provisioning, discovery, monitoring, validation and management 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.

The following sections provide an overview of the certificate, and SSH options available in Venafi Trust Protection Platform. This information provides a conceptual framework which you can use to determine how you want to use Venafi Trust Protection Platform to manage encryption assets in your own organization.

This chapter contains the following topics:

TLS Protect

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.

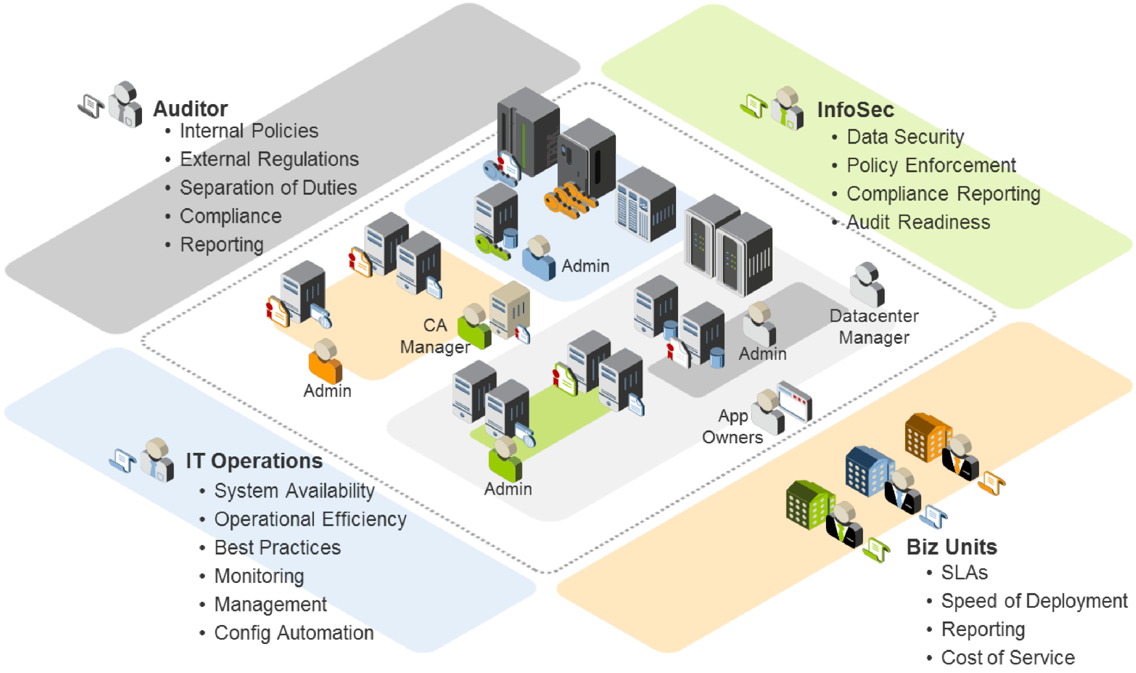
While certificates and their associated private keys are leveraged heavily for mission-critical applications, they come with overhead.

First, the trust and validity of a certificate is time limited–typically valid for one year–and must be renewed before the life-cycle 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.

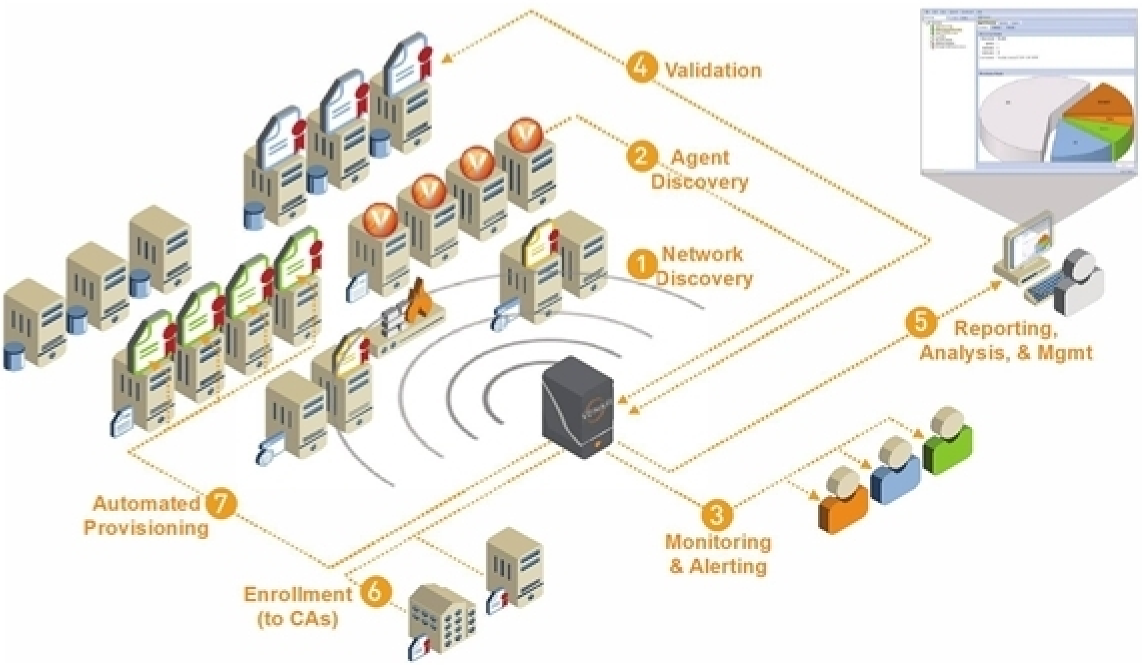
Finally, the certificates and private keys must adhere to current encryption standards and best practices.

Venafi TLS Protect enables organizations to rapidly develop an accurate certificate inventory and identify security and operational risks.



Organizations can quickly evaluate their compliance with corporate and regulatory folders and establish a concise methodology to ensure compliance. With built-in management and policy best practices, Venafi TLS Protect helps eliminate data breaches, security audit failures and unplanned system outages.

Venafi TLS Protect enables organizations to quickly quantify their 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, Venafi TLS Protect provides four levels of certificate management.

- Discovery (1 and 2)
- Monitoring and Validation (3 and 4)
- Enrollment (6)
- Provisioning (7)

Monitoring

At this level, organizations can continuously monitor key and certificate assets for improved inventory and risk mitigation. Venafi 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, Venafi 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, Venafi TLS Protect can validate the certificate is installed and properly configured.

Enrollment

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

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

After the CA signs a certificate, Venafi TLS Protect 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 target systems.

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.

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 How Provisioning Works 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 in the *Trust Protection Platform Certificate Management Guide*.

SSH Server and Key Management

SSH (Secure Shell) is used to secure mission-critical systems such as firewalls, routers, switches, and Unix or Linux systems. To implement SSH, encryption keys are deployed on the server systems and the client workstations that access them. The server and trusted host keys are used to encrypt communications and authenticate systems.

Because of the historically distributed nature of SSH deployments, SSH keys are not typically tracked, rotated or managed. When combined with the large volumes of SSH keys in use, organizations face a myriad of risks and challenges. Poor key management practices leave organizations vulnerable to significant risks including unauthorized access, failed security audits and unplanned system downtime.

Venafi Trust Protection Platform™ lets you quickly inventory your SSH environment, map trust relationships between systems, identify keys that do not meet corporate encryption standards, and locate lost, orphaned, or unused keys.

In order to establish a comprehensive inventory of SSH keys, Trust Protection Platform provides both network and agent-based discovery. 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.

Once Trust Protection Platform identifies the SSH servers, administrators can run agent-based discovery on SSH servers. Agent discovery on the SSH server locates user public keys which, in turn, are used to identify trust relationships with other systems acting as SSH clients.

To complete the picture, administrators can then deploy the agent on the SSH client systems to scan the client’s trusted host files and to determine which hosts the workstation connects to.

All discovery results are correlated at the Trust Protection Platform server to create a comprehensive inventory of SSH keys and their corresponding configuration information. Trust Protection Platform also provides a dependency mapping of all keys and trust relationships. Organizations can then use this information to mitigate security risks, effectively implement a consistent security standard across all supported SSH systems, and ensure critical system availability.

Accessibility features of Venafi Platform

Venafi recognizes the importance of making our products accessible to people of all abilities. We're continually adding features that improve the overall accessibility of our products. In this release, you can benefit from the following accessibility features in Venafi's modern OneVenafi interface.

Keyboard-based navigation

You can use your keyboard to navigate through the product without the use a mouse using standard keyboard navigation conventions.

- Use **TAB** to navigate from one focusable element to the next.
- Use **SHIFT** + **TAB** to navigate to the previous focusable element.
- Use **ENTER** to activate the element that has focus.
- Use the keyboard arrow buttons (**UP**, **RIGHT**, **DOWN**, and **LEFT**) in the following ways:
  - **UP** or **DOWN** to switch between selections in a radio-style user element.
  - **UP** or **DOWN** to scroll the page up and down (if the element with focus is not a menu or a radio group)
  - **PAGE UP** or **PAGE DOWN** to scroll an entire page at a time in the desired direction
  - **RIGHT** or **LEFT** to move cursor one character in the indicated direction.

Additionally, the following accessibility features are available.

- When a page loads, press **TAB** once to see the **SKIP TO CONTENT** option. Pressing **ENTER** will take you to the main section of the page, bypassing menus to make it easier to use the product, especially when you are on the page you need.
- Use the **SPACE BAR** to check (select) or uncheck (deselect) check boxes.

- When navigating the Aperture menus, you can use the following keyboard actions:
  - **UP**, **RIGHT**, **DOWN**, or **LEFT** to navigate through menus and sub-menus.
  - **ENTER** or **DOWN** opens a menu title so you can see its contents.
  - In a sub-menu, **DOWN** and **UP** allow you to navigate through that sub-menu.
  - In a sub-menu, **ESC** closes the sub-menu and takes focus back to the menu title.
  - In a sub-menu, **RIGHT** and **LEFT** close the sub-menu and move you to the adjacent menu titles.
  - In a sub-menu, **UP** to close a drop-down menu.
  - In a sub-menu, **RIGHT** or **LEFT** to exit the sub-menu.
- If you are using the site in small-screen/responsive mode, note the following:
  - You press **ENTER** to activate the hamburger menu, then press **TAB** to navigate the menu.
  - When a menu title has focus, press **ENTER** or **RIGHT** to expand the menu.
  - The **DOWN** key just navigates to the next menu item. It does not expand a sub-menu.
  - The **UP** key expands the current menu item. To navigate to the previous top-level menu item, use **ALT** + **TAB**.
  - To close the menu and return to the page contents, press **ESC**.

Here are some tips for using the search feature in the menu bar:

- Once you have entered at least three characters, the system starts searching, and a box will drop down with a list of matches; as you continue to type, it will refine the search further.
- **DOWN** will enter the drop down list to allow you to navigate through the search results. **ENTER** will take you to the page for the selected object.
- When in the search box itself **ENTER** will bring up a page with all the search results.

On the inventory pages there is a left bar with search filters. When using the search filters:

- As you **TAB** through the available filters, any time you select filter criteria and press **ENTER** (or leave the field), the new filter criteria will be applied and the inventory list will be updated.

- Some filters have a fixed set of options; **ENTER** will bring up the list of available options. You can arrow through them, and press **ENTER** to add the item to the filter criteria. If you want to add another, press **ENTER** again.

Additional accessibility features

- As you press **TAB**, tool tips automatically display if an element has a tool tip. The tool tip is dismissed when you change focus to another item.
- Accessibility features are provided in both standard top-menu mode, as well as in small-screen responsive mode.
- On dashboard pages there are microwidgets. If you want to customized the order of the microwidgets, remove all microwidgets and add them back in the order you want to see them on the screen.

Venafi continues its multi-year process of deprecating features from the older "WebAdmin"-style interface (still seen in *Policy Tree*). Because these features are being migrated to the more modern OneVenafi interface, Venafi does not intend to make any changes to improve the accessibility of the Policy Tree.

As new features are moved from the Policy Tree into the modern interface, and as new features are added to the product, Venafi will continue enhancing the accessibility of the product to ensure people of all abilities can benefit from the product.

If you find areas of the web interface where accessibility can be improved, we welcome your feedback. Please contact Venafi Customer Support at support@venafi.com.

New Inventory accessibility features

Starting in the 20.2 release, Venafi began releasing new inventory tables based on an improved framework. The first inventory to use the new framework is the API Integrations Inventory. In future releases other inventories will be moved to this new framework and will have the same accessibility features.

> **TIP** You can tell if you are using an old inventory page or a new inventory page by looking for the **Density** button at the top of the table. If the **Density** button is there, you are using an inventory based on the new framework. If there is no **Density** button, it's an older table, and the following accessibility features don't apply.

To navigate the inventory using the keyboard:

- Tab to the table by pressing the TAB key to move forward (or SHIFT + TAB to move backwards) until the first column heading has focus.
- When a checkbox has focus, press the SPACE key to select or deselect the row.

When inside the table:

Key	Description
Arrow keys (up, down, right, left)	Navigate between cells.
HOME	Navigate to the first cell in the current row.
END	Navigate to the last cell in the current row.
CTRL + HOME	Navigate to the first cell of the first row.
CTRL + END	Navigate to the last cell of the current row.
SPACE (or PAGE DOWN)	Navigate to the next scrollable page.
PAGE UP	Navigate to the previous scrollable page.
CTRL + A	Select all rows (for multi-row actions).
TAB	Leave table to navigate to next control outside the table
SHIFT + TAB	Leave table to navigate to previous control outside the table.

When a column heading has focus:

Key	Description
ENTER	Cycle through the sort options for that column.
CTRL + SHIFT + ENTER	Open the column's action panel.

Details view. Top open the Details view, navigate to an item in the **Name** column, then press ENTER. Once in the details view:

Key	Description
TAB	Move between controls.
ENTER or SPACE	Activate the control.
Arrow left and	When one of the tabs (like Overview) has focus, use the arrow keys to move between

Key	Description
Arrow right	tabs, then press TAB to move to controls on the tab.
ESC	Close the modal window and return to the previous screen.

5

Management Architecture

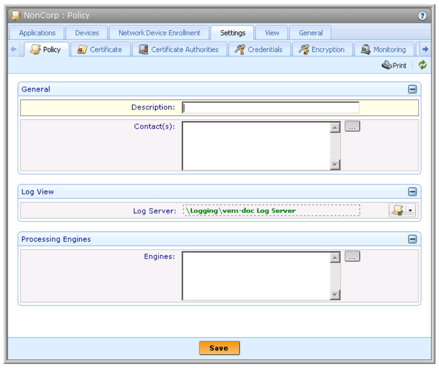
Venafi Trust Protection Platform™ configures and manages all encryption assets–that is, administrative users, groups, credentials, CAs, devices, applications, certificates, SSH servers and keys, and symmetric keys–using objects in a tree-based administrative interface. This object-based management system helps administrators see relationships and dependencies between objects and provides an intuitive framework for deploying security folders and distributing administrative permissions.

The following sections review each component in the Venafi Trust Protection Platform architecture. Each section includes a discussion of how the component relates to other objects, and if applicable, the component's relevance to each level of encryption asset life-cycle management.

This chapter contains the following topics:

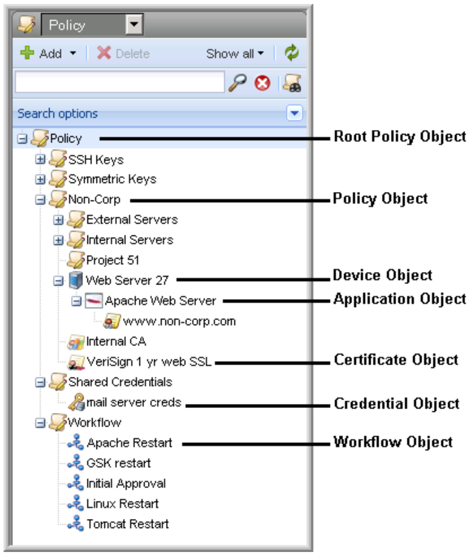
About Policies

Policies provide centralized points of management for objects. Administrators can use policies to manage object configuration parameters, distribute object permissions, and enforce security requirements for objects in the tree. Policies are also used to apply or block Workflows and define parameters for certificate expiration events.



Log Server: \Logging\vem-doc Log Server

Policies can be and managed in the Policy tree. In the Policy tree hierarchy, policies are created only under other policies. Device, CA Template, Certificate, and Workflow objects are created directly under policies.



To apply a policy to system objects, you simply create the objects under the policy. Each time Trust Protection Platform references an asset in the Policy tree, it starts with the root policy at the top of the tree, then reads down through the policy hierarchy until it arrives at the asset. Every attribute you define in a policy is read for all subordinate assets.

This means that policy values are implemented in real time every time the asset is read.

The way in which a policy value is implemented, however, depends on whether the value is locked or not. When Trust Protection Platform looks up an object’s configuration in the tree and it encounters a locked value in a parent Policy, it stops reading down the tree. A locked value is the only value used for all subordinate objects in the tree. It doesn’t matter what is actually configured in the subordinate objects–Trust Protection Platform uses only the first locked policy value in the tree.

If you do not lock a policy attribute, the attribute functions as a default value–that is, it appears as the default option when you create new subordinate objects–but it can be overwritten at the object level. Unlocked policy values flow down the tree with the lowest value taking precedence. That means that when Trust Protection Platform looks up an object’s configuration in the tree and it encounters an unlocked policy value, it continues reading down the tree until it reaches the object configuration. Attributes defined at the object level always take precedence over unlocked values inherited from policies higher up the tree.

In the same way that policies are used to manage object configuration, they can also be used to manage user permissions assignments. In Trust Protection Platform, permissions flow down the tree. This means that when you grant permissions to a policy, all subordinate objects inherit those same permissions unless you explicitly grant different permissions at the individual object level. Policy structure provides a natural framework to distribute system administration. For example, if encryption system assets are managed by locale, you can define local permissions assignment in a policy for each locale. Similarly, if encryption assets are managed by function, you can manage administrative permissions using a policy for each type of encryption asset. Using this model, you assign general permissions at the policy level and specific permissions at the asset level. Using policies to manage permissions assignments simplifies permissions management by providing a central point of control, while still affording the flexibility to assign individual permissions at the object level.

Another way that administrators can use policies to facilitate system administration is in the use of management partitions. Management partitions control which servers provide provisioning and validation services for objects in the Policy tree. If there are multiple Trust Protection Platform servers in your encryption environment, you can assign a different server, or “processing engine,” to each policy. That server will then run the provisioning and validation processes for the policy’s subordinate objects. This functionality is particularly useful in heavily firewalled environments where you want the local server at each site to manage processing for the local certificates and keys.

For information on creating and configuring policies, see Using folders to Manage Encryption Resources in the *Venafi Trust Protection Platform Administration Guide*.

Management Trees in Policy Tree

Venafi Trust Protection Platform manages all encryption system objects in a hierarchical tree structure. The management trees provide an intuitive, centralized point of administration for encryption resources.

There are multiple management trees in the Trust Protection Platform interface. To view a management tree, click the **Tree** drop-down menu, then select the tree you want to view.

Management Trees

Management Tree	Description
Credentials Tree	Credential objects are created and managed in the Credentials tree. Credential objects store the credentials Venafi Trust Protection Platform uses to authenticate with devices, applications, and CAs. Credentials can also be created and managed in the Policy tree. In the Policy tree hierarchy, Credential objects may be contained by Policy, Device, or Application objects. The ability to create Credential objects under different objects in the Policy tree facilitates the distribution of Credential object permissions assignments. For example, if you assign permissions at the policy level, then create the Credential objects under the same policy where their associated applications or certificates are located, the credentials automatically inherit the same permissions as their associated objects. In this way, you can ensure that administrators have permissions to only those credentials required to manage the applications or certificates for which they are responsible. For more information on managing your system credentials, see Managing system credentials in the *Venafi Trust Protection Platform Administration Guide*.
Discoveries Tree	The Discoveries tree lists the configured Discovery and Discovery Exclusion objects for network and agent-based discovery. A discovery allows you to regularly scan a device, a range of IP addresses, a file system, or a local keystore for SSL certificates, client certificates, SSH server keys, and SSH trusted host keys. Each Discovery object in the tree defines the discovery parameters and lists the discovery results. Each Exclusion object in the tree defines ranges of IP 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.

Management Tree	Description
	For more information on configuring and managing discoveries in the Discovery tree, see Discovering certificates and keys in the *Venafi Trust Protection Platform Administration Guide*.
Encryption Tree	The Encryption tree contains your system’s Encryption drivers. Encryption drivers provide access to the keys used to secure your system’s encryption assets–that is, certificates, private keys, SSH keys, Credential objects, administrator user names and passwords, and all other information stored in the Secret Store database. Trust Protection Platform uses either a software key or a hardware key on a supported HSM device (or both) to secure encryption assets within the Secret Store. For more information on managing system encryption, see Managing applications in the *Venafi Trust Protection Platform Administration Guide*.
Identity Tree	In Venafi Trust Protection Platform, all users, groups, and user data stores are managed in the Identity tree. For more information on managing objects in the Identity tree, see Working with Identities & Permissions in the *Venafi Trust Protection Platform Administration Guide*.
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. The Logging tree lists every application that can log events to Venafi Trust Protection Platform. Each Logging Application object, in turn, stores the definitions for its associated events. This is a valuable reference when you are configuring your system notifications. The Logging tree also provides a view of all configured Notification and Channel objects. Notification objects define which types of events you want to monitor and under what conditions. Channel objects define the event output target.

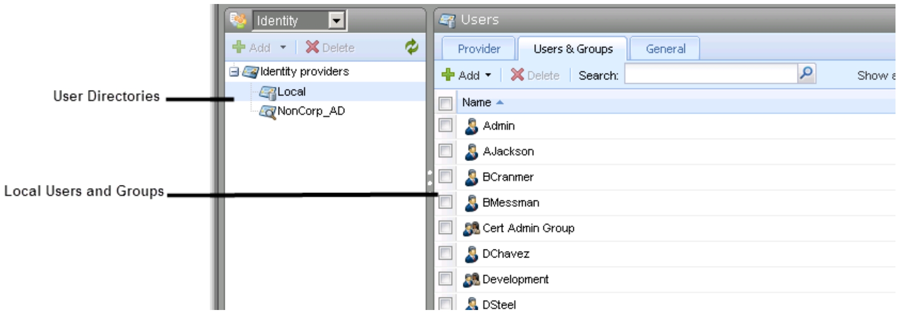
Management Tree	Description
	For more information on managing logging and system notifications, see Understanding system logging and notifications in the *Venafi Trust Protection Platform Administration Guide*.
Platforms Tree	The Platforms tree displays the Venafi Trust Protection Platform servers and modules. For example, if you have your central Director server and a dedicated Discovery Server, this tree displays the two Server objects and their associated modules. From this tree, you can define global module settings like Certificate Renewal and Notification monitoring cycles, the time the Director server runs its daily tasks, and the Discovery schedule.
Policy Tree	The Policy tree provides a hierarchical view of your encryption deployment model. Policy, Jump Server, Device, Application, CA Template, Credential, Certificate, SSH Key, and Workflow objects display in context of other system objects so you can intuitively design your object hierarchy and policy inheritance paths. For information on managing folder, see Using policies to manage encryption assets in the *Venafi Trust Protection Platform Administration Guide*.

Management Tree	Description
Reports Tree	The Reports tree allows you to create and manage system reports. The individual Report objects–Licensing, Entitlement, Expiration and SSH Key reports–determine report format, how often the report is generated, and report delivery options. For more information, see Managing system reports in the *Venafi Trust Protection Platform Administration Guide*.
Roots Tree	The Roots tree lists all archived root and intermediate root certificates in context of their signature chain. From this tree, you can download root certificates to other servers. For more information on managing objects in the Roots tree, see Managing root certificates in the *Venafi Trust Protection Platform Certificate Management Guide*.
Workflow Tree	In the Workflow tree, you create the reason codes you want to associate with Certificate Approval Requests. Reason codes provide customized explanations or instructions for certificate approvers. In Policy Tree, the Workflow tree also allows you to view and manage approval requests. For more information on implementing and managing your corporate workflow procedures, see Implementing Certificate workflow management in the *Venafi Trust Protection Platform Certificate Management Guide*.

Identities

To manage the encryption assets in your security environment, Trust Protection Platform allows you to distribute administrative responsibilities to users and groups called "Identities." You can create Identities in the local Trust Protection Platform database or access existing users and groups from Active Directory (AD).

Trust Protection Platform supports local identities as well as external identities from multiple AD directories and domains.



Name
Admin
AJackson
BCranmer
BMessman
Cert Admin Group
DChavez
Development
DSteel

All users listed in the Identity tree can log in to the Trust Protection Platform management console. However, what they can see and do depends upon their assigned permissions. Trust Protection Platform uses a least privileged model of system administration. So, by default, local users have only the Read permission and external users have no permissions. You must explicitly grant permissions to users before they can manage objects.

In Venafi Trust Protection Platform, all administrative permissions are managed at the object level. On the object Permissions tab, you select the users or groups you want to have permissions to the current object and its subordinate objects, then you select which permissions you want the user or group to have. For further discussion on permissions and permissions inheritance, see "Permissions and abilities" on page 50.

For comprehensive information on managing identities in Venafi Trust Protection Platform, see Working with identities, permissions, and roles in the *Venafi Trust Protection Platform Administration Guide*.

Jump servers

A jump server is an intermediary server through which external agents, such as Venafi Trust Protection Platform, can access a device behind a firewall. If a jump server is required to access devices behind a firewall, the Jump Server object provides the information Venafi Trust Protection Platform needs to communicate with target device via the jump server.

Jump servers can authenticate using either a private key or a user name and password. Jump servers are typically managed over SSH. However, the target device and application cannot use a private key for authentication.

Venafi Trust Protection Platform can both install and extract certificates and private keys through the jump server. Many system operations–including onboard validation–take place via the jump server. Venafi Trust Protection Platform never accesses the jump server's associated application(s) directly.

Jump servers are not supported by all applications. For more information, see Jump server prerequisite configuration in the *Certificate Authority and Hosting Platform Integration Guide*.

When Venafi Trust Protection Platform provisions certificates to servers that require a jump server connection, it securely copies the certificate and private key to the jump server. When the files are no longer needed, Venafi Trust Protection Platform removes the files from the jump server.

Jump Servers are created and managed in the Policy tree. In the Policy tree hierarchy, Jump Server objects are created under folder. Device objects can be created under Jump Server objects.

For more information, see Managing in the *Venafi Trust Protection Platform Certificate Management Guide*.

About devices

Devices represent the physical host on which certificates and private keys are installed. Trust Protection Platform references the device when it validates and manages certificates and private keys.

Device objects are created and managed in the Policy tree. In the Policy tree hierarchy, Device objects are created under folder. Application and Certificate objects are created under Device objects.

For more information on creating and managing Device objects, see Managing Device Objects in the *Venafi Trust Protection Platform Certificate Management Guide*.

About applications

An *application* is an instance of a certificate on a device. It's different from *application software*. In Trust Protection Platform, an *application* occurs when a certificate is placed on a device.

Applications 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 or perform key management functions on the application's associated platform or keystore.

When you create an Application object, you provide all the configuration information Trust Protection Platform needs to manage trust assets on that platform or keystore. Depending on the application, this may include certificate paths and file names, application credentials, private key credentials, and so forth.

Application objects are created and managed in the Policy tree. In the Policy tree hierarchy, application objects are created under device objects. Optionally, certificate objects can be created under application objects.

For more information, refer to Managing applications in the *Certificate Authority and Hosting Platform Integration Guide*.

About credentials

In Trust Protection Platform, *credential objects* provide an innovative way to centrally manage and share your system credentials. Each credential object can be associated with a single device or application, or it can be shared by multiple objects.

Most credential objects store the credentials used by Trust Protection Platform to authenticate with devices, applications, CAs, and Active Directory user directories. Without them, Trust Protection Platform can't manage the certificates associated with devices, applications, and CAs. Other Credential objects don't store credentials but instead connect with external password vaults such as CyberArk or HashiCorp Vault (which can be done using the Adaptable Credential).

You create credential objects in Trust Protection Platform using any of the following credential types:

- Adaptable Credential (*Username/Password*, and *Password*)
- Amazon Credential
- Certificate Credential
- CyberArk Username Private Key Credential
- Generic Credential
- Google Cloud CA Credential
- Password Credential
- Private Key Credential
- Username Password Credential

> **DID YOU KNOW?** The actual credential types you see depends on the products you have licensed.

One of the great things about credential objects is that after you create them, you don't have to repeat the credential configuration for every device, application, or CA. You just reference the existing credential object. If the credential changes–for example, an organization's security policy might require changing user name and password credentials every 90 days; or you might need to swap out a private key used by an existing private key credential–you merely update the single credential object to give Trust Protection Platform access to all of its associated devices and applications.

Credential objects are required at the Provisioning level of certificate management to authenticate with applications, devices, and the CA. Credential objects are also required under Enrollment to authenticate with the CA. For more information, see Managing System Credentials in the *Venafi Trust Protection Platform Administration Guide*.

Credential objects can be created and managed in both the Credentials and Policy trees.

In the Credential tree hierarchy, all credential objects are created under the Root Credential object.

In the Policy tree hierarchy, credential objects may be contained by policy, device, or application objects. The ability to create credential objects under different objects in the Policy tree facilitates the distribution of credential object permissions assignments.

> **EXAMPLE** If you assign permissions at the policy level, then create the credential objects under the same policy where their associated applications or certificates are located, the credentials automatically inherit the same permissions as their associated objects. In this way, you can ensure that administrators have permissions to only those credentials required to manage the applications or certificates they are responsible for.

Policy, device, application, and CA template objects reference credential objects in their respective configurations.

For more information, see Managing System Credentials in the *Venafi Trust Protection Platform Administration Guide*.

Certificate authority (CA) templates

Venafi Trust Protection Platform can submit CSRs and retrieve certificates from many certificate authorities (CA).

In Trust Protection Platform, a CA template object defines the information Trust Protection Platform needs to connect to the CA so it can submit CSRs and retrieve certificates from the CA during enrollment and provisioning operations. The CA template object also defines the template used to post a certificate CSR.

Trust Protection Platform lets you to create multiple CA template objects for each CA, if needed, to support multiple instances, accounts, or configurations of the CA. For example, in the case of Microsoft Certificate Services, you might have separate instances of the CA installed on multiple servers. You would create a separate CA template object to support the individual CA requirements.

You can also create multiple CA template objects for each CA to support different certificate templates. For example, if you want your CA to issue both basic SSL and EV certificates, you must create two different CA template objects—one that issues basic SSL certificates and one that issues EV SSL certificates.

CA template objects are required at the *enrollment* and *provisioning* levels of certificate management. Under certificate enrollment and provisioning, every certificate object must reference a CA template object. Otherwise, Trust Protection Platform cannot issue or renew the certificate.

CA template objects are created and managed in the Policy tree. In the Policy tree hierarchy, CA template objects can be created only within policy folders.

For more information, see Managing CA Templates in the *Venafi Trust Protection Platform Certificate Management Guide*.

Certificates

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

Using Agent Discovery, administrators can discover end entity 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.

Certificate objects are required at the Monitoring, Enrollment, and Provisioning levels of certificate management. For more information on Venafi Trust Protection Platform management levels, see "TLS Protect" on page 20.

Certificate objects are created and managed in the Policy tree. In the Policy tree hierarchy, Certificate objects can be created under Policy or Application objects.

Network Certificates

Venafi Trust Protection Platform simplifies the process of managing network certificates through their life cycles. When a network 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, Venafi TLS Protect interfaces directly with a CA to initiate certificate renewal and key generation requests according to organization-defined workflow and approved folders. After the CA signs the certificate, Venafi TLS Protect 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).

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.

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

If the certificate is configured for Provisioning, Venafi TLS Protect 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 Venafi 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 Venafi 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.

Local certificates

Venafi Trust Protection Platform TLS Protect allows organizations to scan their network’s local file systems and keystores to build an inventory of local certificates—that is end entity certificates as well as root and intermediate root certificates. After you discover your local certificates, you can bring those certificates under management for Monitoring. Discovery is the fastest and easiest way to bring local certificates under management because the Trust Protection Platform automatically populates many certificate settings.

When you bring a local certificate under management, Trust Protection Platform monitors the certificate and provides current information on the certificate status. When a local certificate nears the end of its lifecycle, Trust Protection Platform provides notifications so you can renew and install the certificate before it expires.

For more information, see Managing Local Certificates in the *Venafi Trust Protection Platform Certificate Management Guide*.

Platform Objects

Because of its modular architecture, Venafi Trust Protection Platform can be deployed on a single server as a self-contained system or it can be deployed on multiple servers to distribute specialized functions such as Discovery or Logging. Every time you install Venafi Trust Protection Platform, the program automatically registers the server in the Venafi Trust Protection Platform database. The server then appears as an object in the Platforms tree.

The program modules also appear under every server in the Platforms tree. When you install Venafi Trust Protection Platform, every module is installed on the server. However, the modules may or may not be enabled. During installation, you can select which modules you want to enable on the current server. After install, you can enable or disable modules in the Platform tree. Therefore, if a server performs a specialized function, such as a dedicated Discovery Server, you may enable only a single module on that server.

The Platform modules also enable you to configure program functions. For example, the agent Modules allow you to centrally manage agent configuration. Using the Agent Modules, you can determine the time at which Trust Protection Platform Agents run local discovery scans as well as the time the Agents report their discovery results. Additionally, you can designate the directories or keystores that you want to include or exclude from the discovery scan and the types of files you want to discover.

6

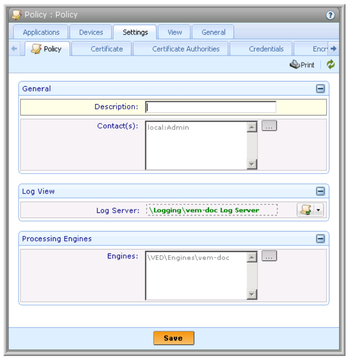
System Management features

The following sections provide an overview of Venafi Trust Protection Platform™ management functionality so administrators can determine how to use Venafi Trust Protection Platform to effectively manage their encryption assets.

This chapter contains the following topics:

Management Zones

Venafi Trust Protection Platform gives administrators the ability to manage which servers provide services for which objects in the Policy tree. This distribution of services is handled at the Policy level. If there are multiple Venafi Trust Protection Platform servers in your encryption environment, you can assign different servers, or “processing engines,” to each Policy object. That server will then run the services for the Policy’s subordinate objects.



General

Description:

Contact(s): local:Admin

Log View

Log Server: \Logging\vem-doc Log Server

Processing Engines

Engines: \VED\Engines\vem-doc

This functionality is particularly useful in WAN environments where you want the local Venafi Trust Protection Platform server at each site to manage processing for the local certificates and keys.

Using management partitions

Segmented and isolated environments sometimes exist. Some are very easy where every Venafi Server can talk to any part of the network. In others, only certain servers can get to the internet. Some environments contain servers that are isolated to network segments, down to a level where every IP address and Port needs to have a rule to pass through a firewall. Some are even trickier still because two data centers exist and both data centers use identical IP addresses.

Examples

Case 1: Limited access to the internet

Customer environments where only one of the three Trust Protection Platform servers in the environment can talk to a CA out on the internet. This server is basically in a security zone and is not allowed to talk freely inside the private network either.

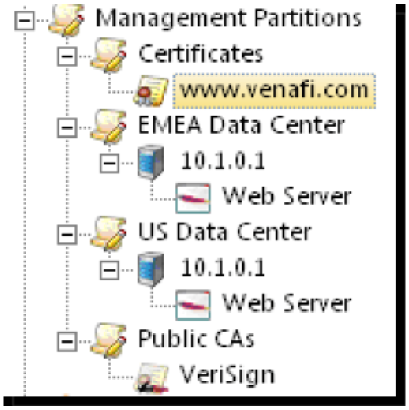
Case 2: Isolated network segments

Not all Trust Protection Platform servers have the ability to talk to every target machine in the environment.

Case 3: Duplicate data centers

When two identical data centers exist and failover protection is needed. Everything is identical in this environment, including the IP addresses, which makes managing this environment tricky.

All three of these cases can be represented with this policy tree structure:

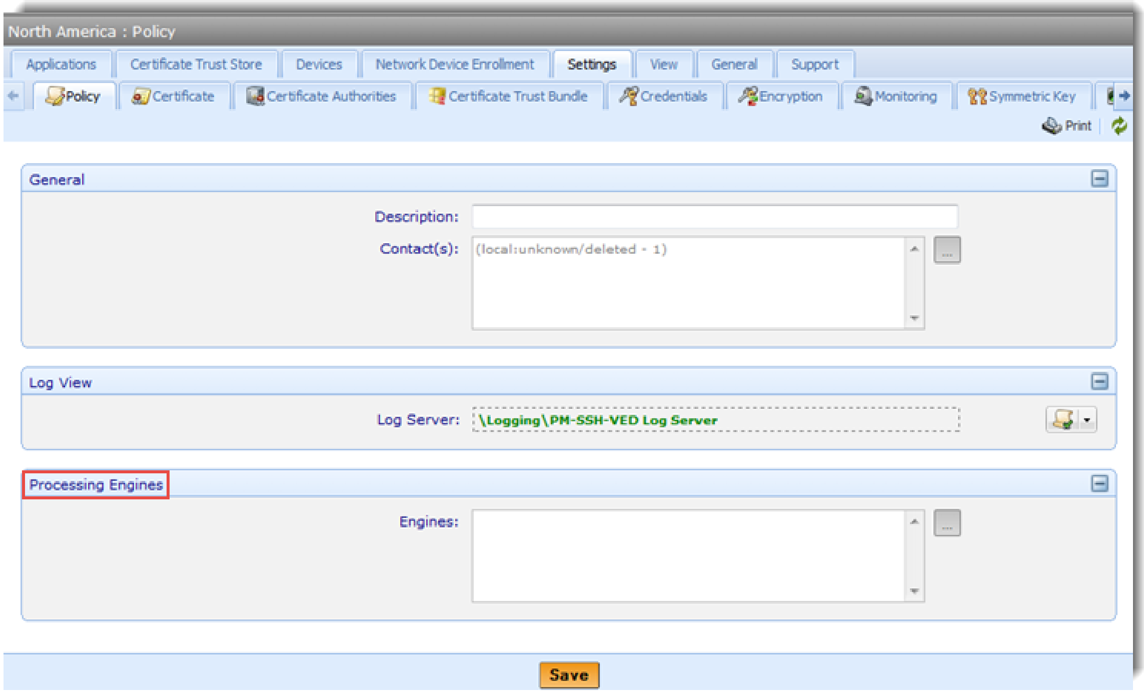


Management Partitions
- Certificates
  - www.venafi.com
- EMEA Data Center
  - 10.1.0.1
    - Web Server
- US Data Center
  - 10.1.0.1
    - Web Server
- Public CAs
  - VeriSign

To solve this issue

Scenario

If you look at a the Policy section in the Policy Tree, you'll see a section called *Processing Engines*. By default, this configuration is empty, which means that any Trust Protection Platform engine can process objects within that folder and below.



Description:

Contact(s): (local:unknown/deleted - 1)

Log Server: \Logging\PM-SSH-VED Log Server

Engines:

If you specify one or more Trust Protection Platform engines in that configuration only those engines can process objects in that policy folder and below.

Now, if you have three Trust Protection Platform servers in your environment with the following names and restrictions:

1. DMZ Trust Protection Platform- Can only connect to systems in the Public internet, but also has firewall rules allowing it to connect to the database.

2. Data Center A Trust Protection Platform- Can only talk to Data Center A

3. Data Center B Trust Protection Platform- Can only talk to the Data Center B

Configure the folders in this way:

For certificates in Data Center A and Data Center B:

- If the certificates have private keys generated by the Trust Protection Platform, then all that is needed is a Trust Protection Platform server that can access the DB to generate the Private Key and CSR for the certificate. In this case, either Data Center A or Data Center B server can process the certificate.

- The DMZ Trust Protection Platform server should not process the certificate because you do not want the Private Keys to be generated outside of the protected network.

For devices in Data Center A

- Only the Data Center A server has the ability to access Data Center A for certificate installation and validation purposes.

For devices in Data Center B

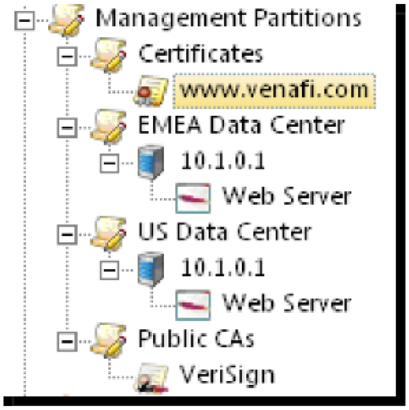
- Only the Data Center B server has the ability to access Data Center B for certificate installation and validation purposes.

Public CAs – DMZ Trust Protection Platform

- Only the DMZ Trust Protection Platform server has access to the Internet to talk to Symantec.

About renewing the ‘www.venafi.com’ certificate

Here is the example screenshot.



Management Partitions
Certificates
www.venafi.com
EMEA Data Center
10.1.0.1
Web Server
US Data Center
10.1.0.1
Web Server
Public CAs
VeriSign

- Set the certificate for renewal. See Scheduling a certificate renewal in the *Certificate Management Guide* for more information.
  - Certificate work:

    Between stages 0 and 400, the certificate object is being processed by either the Data Center A or Data Center B server.

    Keys off of the certificate object if central gen, keys off of the application object if remote key gen.

- Enrollment work:

  Between stages 500-700 , the CA object is effectively being interacted with, which means the Data Center A or Data Center B server will stop working on the job and the DMZ server will pick it up.

  Keys off of the CA template assigned to the certificate object.

- Provisioning work:

  Between stages 800-1200, the Certificate is being provisioned to the Application, which means the Data Center A or Data Center B server will process the job for the appropriate data center.

  A separate Provisioning To Do is created for each application object associated with the certificate. Partition Management keys off of each application object.

- Revocation work:

  Stage 1400.

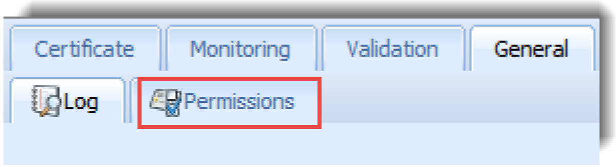
  Keys off of the CA template chosen to perform the revocation and favors by evaluating the Issuer to figure out which CA template to use. Partition management keys off of the CA template.

> **NOTE** For more information about stages, see Workflow object settings in the *Certificate Management Guide*.

> **IMPORTANT** CDP Monitoring and Revocation Checking does *not* honor engine partitioning in the Policy tree.

Permissions and abilities

In Venafi Trust Protection Platform™, all administrative permissions are managed at the object level. Every encryption system object–folders, credentials, workflows, CAs, devices, applications, certificates, symmetric keys, SSH server keys, SSH client keys, notifications, channels, logging applications, and discoveries–has a **Permissions** tab. On the object **Permissions** tab, you select the users or groups you want to have permissions to the current object and its subordinate objects, then you select which permissions you want the user or group to have.



In the Policy Tree, permissions assignments are updated the next time the affected user logs in to the console or when the user clicks Refresh 🔄 in a grid or tree view.

Object permissions

Permission	Allows the user to...
View	The user can see the object in the tree, but cannot select the object or read the values.
Read	The user can see and select the object in the tree. Additionally, the user can read the object data, but no buttons are enabled; the user cannot edit or manage the object. In Certificate objects, users with *Read* permissions to the certificate can see only the associated applications to which they have *View* or higher permissions to the Application object. In Application objects, users with *Read* permissions to the application can see only the associated certificate if they have *View* or higher permissions to the Certificate object. For SSH keysets, users with *Read* permissions to the keyset (if in a policy folder) can view all keys in the keyset. If the keyset is not in a policy folder, then the user can see all the keys in the keyset if they have *Read* permissions on all devices in the keyset.
Write	The user can edit and modify object attributes. To edit an object or its properties, you must have Write permission on the object. Note that if View permission is not granted to the device object where the application is created, the Install button will not be available for the user in Aperture.

Permission	Allows the user to...	
	To move objects in the tree, the user must have *Write* permissions to the objects and *Create* permissions to the target folder. *Read* permissions are inferred. Rename is selected by default but can be deselected. In Certificate and Application objects, the user also has access to the following options in the designated pages:	
	Certificate Summary Page	Users with *Write* permissions to the Certificate object have access to the Restart, Retry, Reset, and Revoke options.
	Certificate Settings Page	Users with *Write* permissions to the Certificate object have access to the Renew Now option.
	Certificate Associations Page	Users with *Write* permissions to the Certificate object can see all associated applications, regardless of their permissions to the individual applications. Users with *Write* permissions to the Certificate object can add associations only to those applications to which they have either *Write*, or both *Associate* and *View* permissions. Users with *Write* permissions to the Certificate object have access to the Retry Installation option only for those applications to which they have either *Write* or both *Associate* and *View* permissions.

Permission	Allows the user to...	
		Users with *Write* permissions to the Certificate object can push the certificate and private key only to those applications to which they have either *Write* or both *Associate* and *View* permissions. Users with *Write* permissions to the Certificate object can enable or disable the certificate only on those applications to which they have either *Write* or both *Associate* and *View* permissions.
	Application Settings Page	Users with *Write* permissions to the Application object can add associations only if no certificate is currently associated with the Application object or if they have either *Write* or both *Associate* and *View* permissions to the associated Certificate object. Users with *Write* permissions to the Application object have access to the Retry Installation option only if they have either *Write* or *Associate* and *View* permissions to the associated Certificate object. Users with *Write* permissions to the Application object can push the certificate and private key to the application only if they have either *Write* or *Associate* and *View* permissions to the associated Certificate object.
	For SSH keys, users with *Write* permissions to a keyset can rotate keys, delete keys from a keyset, add a new key, and can add a passphrase to a key. However, if the user doesn't have *Write* permissions to write to the key's associated device, then the user cannot add keys.	

Permission	Allows the user to...
Create	The user can create subordinate objects, such as devices and applications. *View* is inferred. For SSH keys, you must have the *Create* permission in the target folder to move a keyset into that folder.
Manage Policy	Lets users modify policy values on folders. *Read* and *Write* permissions are implied; the *View* permission is not. In order for the Manage Policy permission to be useful, users should be granted the *View* permission, as well. For SSH keys, you must have the Manage Policy permission in the target folder to move a keyset into that folder.
Delete	Lets the user delete objects. For SSH keys, you need to have the *Delete* permission to remove keysets from all folders (returning the keyset to device-level permissions). For SSH keys, you need the *Delete* permission in the source folder when moving a keyset from one folder to another.
Rename	Lets the user rename objects or move them within the tree. To move an object, the holder must have the *Create* permission in the target location. When an object is moved, locked policy attributes are recalculated.
Associate	If you have *Write* permissions to a Certificate object and both *Associate* and *View* permissions to the application(s) where the certificate is installed, you can perform the following functions in the Certificate object's Certificate Associations page: ▪ Associate or disassociate the application with the certificate ▪ Push the certificate and private key to that application

Permission	Allows the user to...
	- Retry the certificate installation - Enable or disable the processing of certificates on the application. When you disable processing, Trust Protection Platform does not attempt to install, renew, process, or validate certificates for the current application. If you have *Write* permissions to an Application object and *Associate* and *View* permissions to the certificate installed on the application, you can perform the following functions in the Application object's Settings page: - Associate or disassociate the certificate with the application - Push the certificate and private key to that application - Retry the certificate installation This permission is relevant only to Policy, Application and Certificate objects. To associate an object with another object, you must have View permission on both objects. Additionally, to push a certificate to an installation, a user must also have View permissions to the device object where the application is created. Note that if View permission is not granted to the device object where the application is created, the Install button will not be available for the user in Aperture.
Revoke	Revoking a certificate makes it invalid. You must have *Write* permissions to the certificate. Once you Revoke a certificate, you cannot undo the action.
Private Key Read	You can download the private key from the Trust Protection Platform database, if the key is archived in the Trust Protection Platform database. This permission is relevant only to Policy and Certificate objects.
Private Key Write	You can upload a certificate private key file to the Trust Protection Platform database.

Permission	Allows the user to...
	This permission is relevant only to Policy, Certificate, and Private Key Credential objects.
Admin (Policy Tree only)	Grant other user or group Identities permissions to the current object or subordinate objects. In the Aperture console, this permission is called *Manage Permissions*.
Manage Permissions (Aperture console only)	Grant other user or group Identities permissions to the current object or subordinate objects. In Policy Tree, this permission is called *Admin*.

> **NOTE** The master administrator (created in the local Identity Provider during installation) and any accounts granted the master admin role have all permissions to every object in the tree. You cannot remove permissions from the master admin. The user account used to authenticate with an external directory (Active Directory) is also granted master admin 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.

Permissions Inheritance

Permissions flow down the tree. This means that when you grant permissions to an object, all subordinate objects inherit those same permissions unless you explicitly grant permissions to objects further down the tree—in which case, permissions inheritance is determined as follows:

- Permissions assigned to users override permissions assigned to groups.
- Group permissions are cumulative. This means that if there are multiple group assignments, an object’s inherited permissions resolve to the combined group permissions.

Because permissions are inherited from parent objects, one of the best ways to distribute and manage permissions assignments in Trust Protection Platform is through folder. When you grant permissions to a Policy object, all subordinate objects inherit those same permissions unless you explicitly grant different permissions at the individual object level. Policy structure provides a natural framework to distribute system administration. For example, if encryption system assets are managed by locale, you can define local permissions assignment in a Policy object for each locale. Similarly, if encryption assets are managed by function, you can manage administrative permissions using a Policy object for each type of encryption asset. Using this model, you assign general permissions at the policy level and specific permissions at the object level. Using folder to manage permissions assignments simplifies permissions management by providing a central point of control, while still affording the flexibility to assign individual permissions at the object level.

How network discovery works

From the Jobs page, you can create different types of discovery jobs that help you automate the discovery and placement of network certificates and SSH keys. For example, you can create network discovery jobs to get a complete list of your network certificates and SSH keys.

Use Venafi Platformto create the following types of discovery jobs:

- **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 bulkin 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 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 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 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 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 *Overview 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 23.
>
> You can also import certificates from a certificate authority (CA). To learn more, see Importing certificates from a certificate authority in the *Certificate Management Guide*.

Frequently asked questions

Q. What is the network load during discovery?

A. Visit our Support article at https://community.cyberark.com/s/article/Info--Network-load-for-Discovery.

Q. How do I configure the Discovery module settings?

A. Visit our Support article at https://community.cyberark.com/s/article/Info--Configuring-Discovery-Module-settings.

Agent-based discovery

The Server Agent is a client/server application that allows you to discover encryption assets on any supported system in your network. Currently, the agent discovers SSH client keys, SSH Server Keys, and SSL certificates and keys.

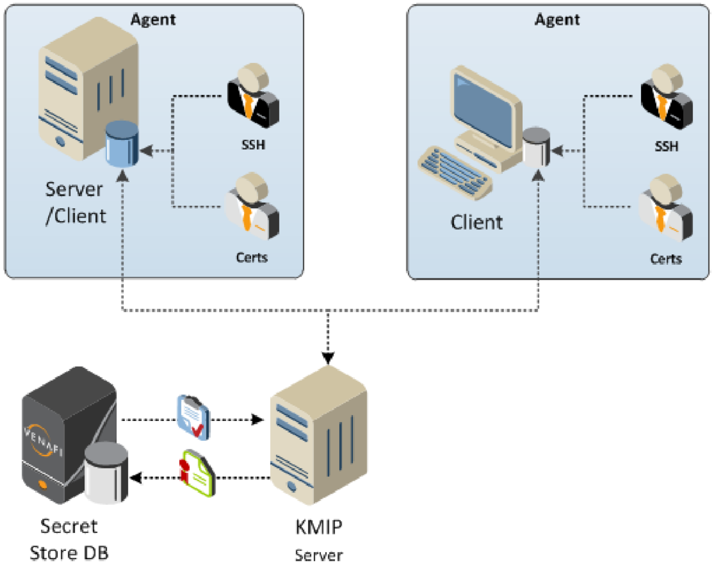
The agent application is installed on local systems–either workstations or SSH servers–where it performs scheduled scans of directories for encryption assets. You can determine the time at which the agent runs its scan as well as the time that it reports the discovery results back to the Trust Protection Platform server. You can configure the agent centrally using the Policy Tree, or at the local level using a command line interface.

When the agent completes a discovery scan, it waits until its scheduled time to check in with the Trust Protection Platform server, then uploads encryption assets to the Secret Store where they can be brought under management and monitored.

The agent provides schedules for SSH key scans. You can determine when each scan occurs and when the Server Agent uploads the results to the Trust Protection Platform server. The ability to individually manage the SSH key scan cycles allows administrators to load balance agent discovery and manage network traffic.

> **DID YOU KNOW?** Server Agent discoveries operate independently of Network Discovery (and vice versa). The difference between Network and Agent Discovery is that Network Discovery can only discover certificates or SSH keys that respond to SSL or SSH queries on designated IP addresses and ports, whereas the agent can discover encryption assets in the file system.

The following diagram provides a visual representation of the Server Agent program components and how they operate in your network environment.



About validation

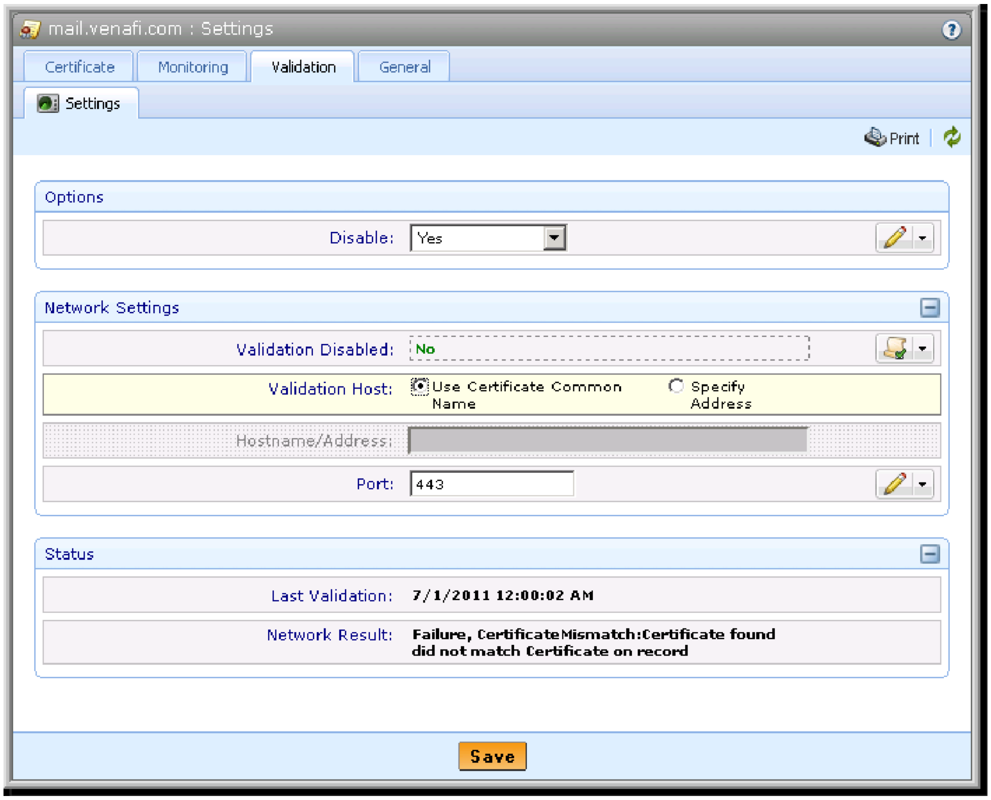
Venafi Trust Protection Platform provides two levels of system validation: Network Validation and Onboard Validation.

Network Validation requires network access from the Trust Protection Platform server to the server where the managed certificates or SSH keys are installed. During the Network Validation process, Trust Protection Platform sends an SSL or SSH request to the target server.

If the server responds to the SSL request, Trust Protection Platform retrieves the certificate serial number and compares it to the certificate Venafi Trust Protection Platform has archived for the corresponding Certificate object. The purpose of Network Certificate 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.

If the server responds to the SSH request, Trust Protection Platform retrieves the SSH server key's information and compares it to the server key Venafi Trust Protection Platform has archived for the corresponding SSH Server Key object. Network Validation on SSH servers allows administrators to determine whether the servers keys are configured in compliance with corporate folders, including key lengths, protocol versions, supported authentication methods and other information.

Network Validation is available for Application, Certificate, and SSH Server Key objects. If you enable Network Validation on a Certificate object and select the **Use Certificate Common Name** option, Trust Protection Platform does a DNS lookup of the certificate's common name. It then validates the certificate at the first IP addresses returned from the DNS lookup.



Options

Disable: Yes

Network Settings

Validation Disabled: No

Validation Host: ● Use Certificate Common Name ○ Specify Address

Hostname/Address:

Port: 443

Status

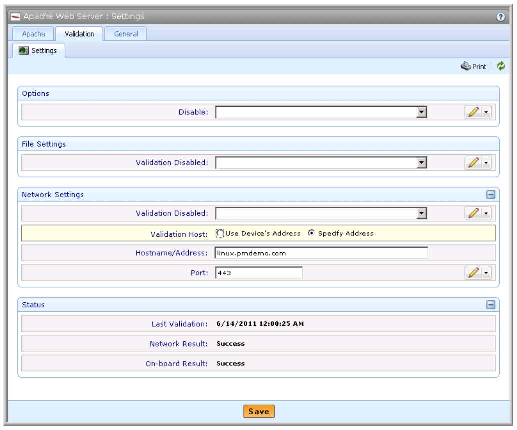
Last Validation: 7/1/2011 12:00:02 AM

Network Result: Failure, CertificateMismatch:Certificate found did not match Certificate on record

If you enable Network Validation on the Application object, Venafi Trust Protection Platform validates the certificate associated with the Application object. Likewise, if you enable Network Validation on an SSH Server Key object, Venafi Trust Protection Platform validates the SSH server key associated with the SSH Server Key object.

Onboard Validation can be enabled only on Application objects. During Onboard Validation, Trust Protection Platform uses the information defined in the Application object to authenticate with the server and to locate the installed certificate. It then compares the installed certificate serial number to the certificate Venafi Trust Protection Platform has archived for the application’s corresponding Certificate object. Onboard Validation is performed using the application’s supported management protocol.

Figure 6.1: Application Object–Network Validation and Onboard Validation Configuration



Disable:

Validation Disabled:

Validation Disabled:

Validation Host: ○ Use Device's Address ● Specify Address

Hostname/Address: linux.pmdemo.com

Port: 443

Last Validation: 6/14/2011 12:00:25 AM

Network Result: Success

On-board Result: Success

The purpose of Onboard Validation is to determine if the Application object configuration is correct and to verify that the correct certificate is installed on the server. If Trust Protection Platform can authenticate with the server, it knows the Application object’s credentials are correct. If it can locate the certificate, it knows the Application object’s certificate configuration is correct. Finally, when it retrieves the certificate serial number, it can determine if the correct certificate is installed.

When you enable Network or Onboard Validation, the Validation Manager module runs daily validation checks and reports the results on the object Validation tab. In addition to reporting validation results on the Application, Certificate, or SSH Server Key object’s Validation tab, Trust Protection Platform generates a validation result event.

For information on validating certificates and the platforms or keystores on which they are located, see Validation Overview in the *Venafi Trust Protection Platform Certificate Management Guide*.

System notifications 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.

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 MSSQL channels provide the information required to write events to a log store.

In addition to the routing channels, Venafi Trust Protection Platform also provides a Filter channel that allows you to filter out events based on event type or severity so you can control what types of events are logged or reduce the number of events logged to a database. The Filter Channel object functions as a sort of intermediary channel. When the Filter channel is selected as the Default Log Channel or the target of a Notification Rule, it filters out the blocked events or severities, then forwards all unfiltered events to a standard routing channel.

Notification and Channel objects 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. It includes the Log server, Log Applications, Channels, and Notifications folders with their associated objects. The following sections review these components. For more information, see Managing System Logging and Notification in the *Venafi Trust Protection Platform Administration Guide*.

This chapter contains the following topics:

Venafi Log server

The Venafi Log server manages the flow of information to and from the log store. The Log server receives incoming events and requests from logging applications, logs information to the log store, and provides selective logging and notification services.

Event Definitions folder

The Event Definitions folder contains an object for every system component that can send events to the Venafi Trust Protection Platform log server. This includes all supported platforms, keystores, and CAs.

Channels folder

The Channels folder contains an object for every configured channel. The Default SQL Channel object defines the default log store. All system events are logged to the Default SQL Channel so you have a comprehensive, auditable log that meets corporate and government audit standards.

Supplementing the default log store, Venafi Trust Protection Platform supports File, Filter, SMTP, SNMP, MS SQL, and Syslog channels. You can use these Channels to provide targeted logging and notifications.

Folder for Notification rules

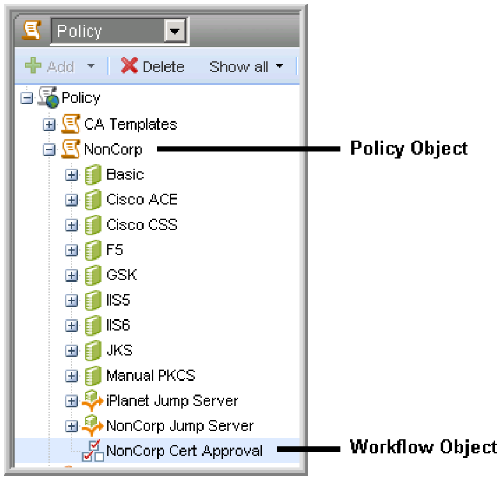
The Notification Rules folder contains Notification objects. Notification objects store the criteria the Venafi Log server uses to select system events. They also designate which Channel objects the Log server uses to provide event responses.

Workflow management

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.

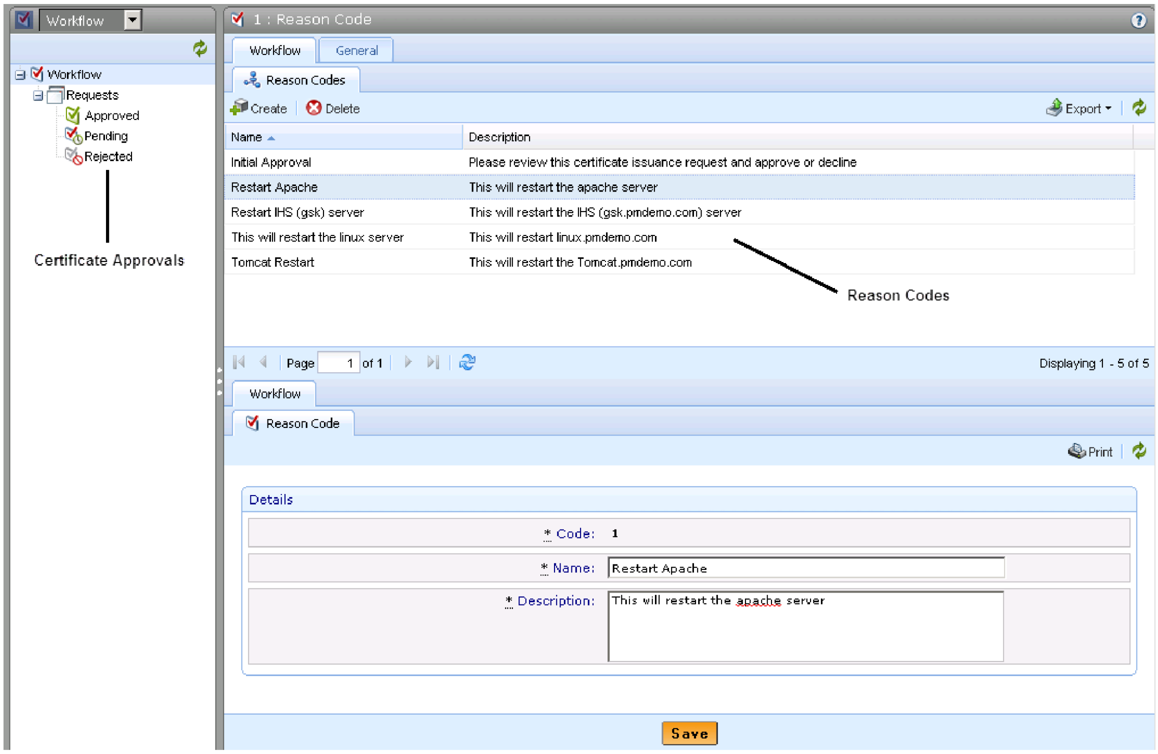
> **NOTE** Trust Protection Platform is able to run local SSH commands only against the following applications: Apache, GSK, IIS5, iPlanet, JKS, PEM, PKCS#12, and Tealeaf PCA.

Application Workflows are defined in Workflow objects, but applied via folder. Workflow and folder are created and managed in the Policy tree. In the Policy tree hierarchy, Workflow objects are created under folder.



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.

Although Approval Reason Codes are selected in Workflow objects in the Policy tree, the Reason Codes themselves are defined in the Workflow tree. In the Workflow tree, you define the Approval Reason Codes that you want to reference in Workflow objects.



Name	Description
Initial Approval	Please review this certificate issuance request and approve or decline
Restart Apache	This will restart the apache server
Restart IHS (gsk) server	This will restart the IHS (gsk.pmdemo.com) server
This will restart the linux server	This will restart linux.pmdemo.com
Tomcat Restart	This will restart the Tomcat.pmdemo.com

* Code: 1
* Name: Restart Apache
* Description: This will restart the apache server

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.

Workflow objects may be used at the Enrollment or Provisioning levels of certificate management to manage your organization’s certificate approval process or interject SSH commands at specific points of the certificate lifecycle. For more information, see Implementing certificate workflow management in the *Venafi Trust Protection Platform Certificate Management Guide*.

Asset encryption

Venafi Trust Protection Platform maintains all system information–that is, configuration settings, managed server and certificate information, credentials, archived certificates, and private keys–in a database. To secure this information, Trust Protection Platform uses encryption, either through a software encryption key, or a hardware encryption key (or both).

To secure the encryption assets within the database, Venafi Trust Protection Platform also encrypts certificates, private keys, Credential objects, administrator user names and passwords, and all other information stored in the Secret Store database. By default, Trust Protection Platform uses the encryption key to secure encryption assets within the Secret Store. However, you can also access AES encryption keys on supported HSM devices to secure encryption assets in the Secret Store.

Encryption drivers provide the information required to access encryption keys in Venafi Trust Protection Platform. Encryption drivers are created and managed in the Venafi Configuration Console.

You can see enabled encryption drivers on the Encryption tree menu in the Policy Tree.

The Software and Null Encryption drivers are provided by default. The software key is Venafi Trust Protection Platform’s default encryption key. It is an AES-256 key stored in the Windows registry. The Null encryption driver actually provides no encryption key at all. It gives users the option of selecting no encryption for objects that do not need to be secured, such as certificates.

If you want to use AES keys stored on a supported HSM device, you must first configure the device connection, then create a PKCS#11 Encryption Driver object in the Venafi Configuration Console.

After you configure the device connection and create the PKCS#11 encryption driver object in the Venafi Configuration Console, you can select the driver’s corresponding encryption keys to define your system’s encryption key settings.

For more information on creating encryption drivers and defining your system’s encryption key settings. see Managing System Encryption Keys in the *Venafi Trust Protection Platform Administration Guide*.

Reporting

Trust Protection Platform provides reporting functionality to help administrators more effectively manage their encryption environment.

The Report objects in the Reports tree provide the information that the Reporting module requires to generate each report. They determine report format, how often the report is generated, and report delivery options.

Trust Protection Platform provides the following default reports.

- The **Certificate Authority Report** contains details related to certificate authorities (CA).

  For detailed information on this report, see Certificate Authority report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Certificate Inventory Report** provides an overview of critical information and statistics about the certificates in your environment so that you can detect anomalies or issues and respond in order to secure and protect your environment.

  For detailed information on this report, see Certificate Inventory report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Certificates with Identical Attributes Report** shows user, device, and server certificates that share an identical attribute with at least one other certificate.

  For detailed information on this report, see Certificates with Identical Attributes report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Entitlement Report** shows all users that have access to the encryption management system.

  For detailed information on this report, see Entitlement report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Expiration Report** contains details about the upcoming expiration dates of your certificates. Expiration dates are displayed from most urgent to least urgent, as defined when the report was generated.

  For detailed information on this report, see Expiration report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Key Length Report** contains details about key lengths of the certificate group you specified. Key lengths are sorted in relative order, from short (weak) to long (strong). This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Key Length report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Licensing Report** provides a count of all managed certificates and their associated applications as well as managed SSH and symmetric keys so administrators can determine if they are in compliance with their current licensing agreement. This report is provided as a default object in the Reports tree because Trust Protection Platform uses the data from the Licensing Report to populate the License Status tab in the administration console Dashboard.

  For detailed information on this report, see Licensing report in the *Venafi Trust Protection Platform Administration Guide*. .

- The **Signing Algorithm Report** contains details related to Digital Signature Algorithms (signing algorithm). The details will help you evaluate risk and company security policy compliance. The algorithms have been sorted in relative order, from weak to strong. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Signing Algorithm report in the *Venafi Trust Protection Platform Administration Guide*.

- The **Validity Period Report** contains shows validity periods for your certificates for the purposes of compliance. The number in the "Years" column reflects the total validity period of the corresponding certificate, not the time remaining. Validity periods are sorted in relative order from long to short, measured in years. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Validity Period report in the *Venafi Trust Protection Platform Certificate Management Guide*.

- The **Wildcard Report** contains details about the use of wildcard certificates. Wildcard certificates are displayed in the table and include the total number of instances and detail associated with each instance. These certificates are sorted by number of instances, from greatest to fewest. This report applies to Network discovery objects only and not to Agent discovery objects.

  For detailed information on this report, see Wildcard report in the *Venafi Trust Protection Platform Certificate Management Guide*.