Venafi Trust Protection Platform v23.1 Common Criteria Guidance

Acumen Security, LLC.

Document Version: 1.0

Table Of Contents

Revision History

Version	Date	Description
0.1	April 2023	Initial document created.
0.2	July 2023	Incorporated Vendor updates for known bug fix.
0.3	October 2023	Updated as per AAR comments, updated SSH supported algorithm list. Added a note in “TOE updates” section. Added configuration steps for Password based and public key based authentication. Added CRL check and verification mode configuration. Added registry setting for common criteria compliant. Added section “TOE patches” to show steps for applying a hotfix.
0.4	January 2024	Added section 8 “Secure Acceptance of TOE”.
0.5	February 2024	Updated as per STv1.2
0.6	May 2024	Added Section 9 “Security Functions provided by the TOE”
1.0	June 2024	Final version for submission.

1 Overview

This document is a guide to Venafi's implementation of the Common Criteria Protection Profile for Application Software, Version 1.4 (2021.10.18) for its Trust Protection Platform Version 23.1 software.

1.1 Evaluation Platforms

Certification has been performed on a platform with an Intel Xeon processor running Microsoft Windows Server 2016 Standard Evaluation [10.0.14393 Build 14393] (referred to hereafter as Windows Server 2016) in FIPS mode running. Windows Server 2016 must have the following packages installed:

- Microsoft .NET Framework 4.7.2
- ASP .NET 4.6
- URL ReWrite Module 1.2
- Universal C runtime

and the following Microsoft Internet Information (IIS) web server roles must be installed:

- Common HTTP Features\Static Content
- Common HTTP Features\Default Document
- Health and Diagnostics\HTTP Logging
- Health and Diagnostics\Logging Tools
- Health and Diagnostics\Request Monitor
- Health and Diagnostics\Tracing
- Security\Request Filtering
- Performance\Static Content Compression

1.2 Technical Support

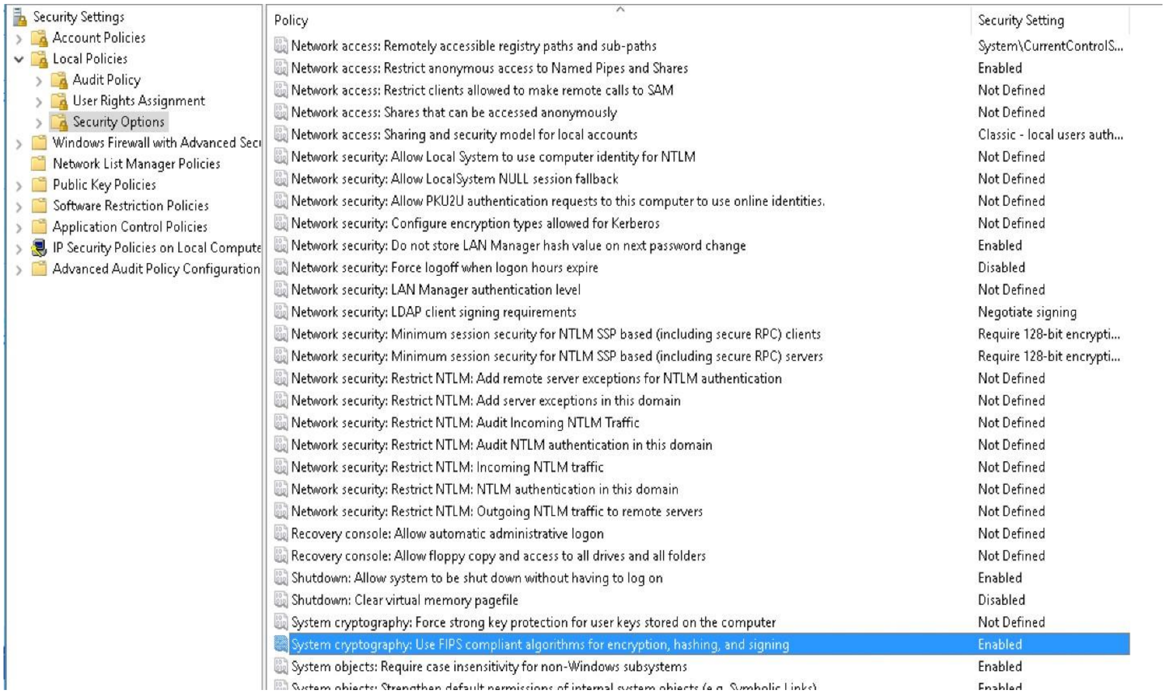
For comprehensive product information, refer to the relevant Venafi product documentation.

2 Platform Configuration

Because the product relies on the underlying cryptographic functionality of the Windows Server platform, Windows Server 2016 must be in FIPS mode to restrict its ciphers to Common Criteria requirements. This can be done through the Local Security policy configuration as follows:

- Open Local Security Policy
- Security Settings > Local Policies > Security Options
- Change the security setting for “System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” to **Enabled**

As shown in the screenshot below:



Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Firewall with Advanced Secu
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration

Policy	Security Setting
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

The platform provides support for the following TLS 1.2 cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

Because this product leverage’s the Windows Server 2016’s Bitlocker full disk encryption functionality, Bitlocker must be enabled in order for the TOE to meet data at rest protection requirements.

2.1 Common Criteria Configuration

To configure the TOE to only use Common Criteria-compliant SSH algorithms, the following registry key needs to be added in registry at HKEY LOCAL MACHINE\SOFTWARE\Venafi\Platform .

Administrator can either create a new dword key as follows directly in the registry at HKEY LOCAL MACHINE\SOFTWARE\Venafi\Platform, or save the following in a plain text file (using a program such as Notepad), save it as a .reg file, and double click to apply it.

```
--------------------------------------------------------------------------------
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SOFTWARE\Venafi\Platform]
"Common Criteria Compliant"=dword:00000001
--------------------------------------------------------------------------------
```

2.2 Database Configuration

The TOE also uses an external database to store credentials, certificates, keys and log data. Microsoft SQL Server 2022 Developer is used in the evaluated configuration. This database can be a local database running on the same host platform or a remote database.

Upon installation of Microsoft SQL Server 2022, configuration of the “database owner” user and the limited “operations user” is required. The database owner account is used only for installation, upgrades, and administrative maintenance. The operations user database account is a limited account used for everyday operations.

The database should be configured to support TLS v1.2.

Please refer to Section 3.3 on instructions to configure the TOE to connect with this configured database.

3 Product Configuration

Venafi Trust Protection Platform provides three consoles for management:

- A web-based console that can be launched by connecting to the TOE using a browser. This web console provides two experiences:
  - OneVenafi - this is the modernized experience that is also referred as Aperture.
  - Policy Tree - this is the classic experience that is also referred as WebAdmin. This experience is gradually being retired as features are moved to the OneVenafi experience. Most of the features in this experience are configuration and administrative activities.
- Venafi Configuration Console (VCC): A powerful Microsoft Management Console (MMC) is a snap-in console that allows you to administer the settings of the Venafi Platform installation. VCC allows you to control Venafi services, enable product components, configure database settings.
- WinAdmin: A Windows-based console that runs locally on the Trust Protection Platform server. Most features from WinAdmin have been moved to the web consoles or to Venafi Configuration Console.

The following items are taken from a Venafi checklist for configuring Trust Protection Platform. They are needed to make the product usable and to place it into a Common Criteria evaluated configuration.

3.1 Define User Data Stores and Identities

To manage keys and certificates throughout your environment, Trust Protection Platform allows you to delegate certificate administration to user and group identities. You can use existing users and groups from Active Directory, or you can create users and groups in the local Trust Protection Platform database.

3.2 Manage Administrative Permissions for System Objects

The first time you log in to Venafi Platform, you must use the default master administrator role (admin). The password for this account is defined during installation.

3.2.1 Permissions Overview

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

In Trust Protection Platform, all administrative permissions are managed at the object level. Every encryption system object—folders, Credentials, Workflows, CAs, Devices, Applications, Certificates, Notifications, Channels, Logging Applications, Discoveries, and Discovery Surveys—has a permissions tab. From the object permissions tab, you select the users or groups you want to have permissions to the current object and its subordinate objects, then you select which permissions you want the user or group to have.

Available Permissions

The following table provides an explanation of the available 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.

Write	The user can edit and modify object attributes. To move objects in the tree, the user must have Write permissions to the objects and Create permissions to the target folder. 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 • Certificate Settings Page • Certificate Associations Page • Application Settings page
Create	The user can create subordinate objects, such as devices and applications. View is inferred.
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.
Delete	Lets the users delete objects.
Rename	Lets the user rename objects or move them within the tree. To move an object, the holder must have the Create permission in the target location. When an object is moved, locked policy attributes are recalculated.

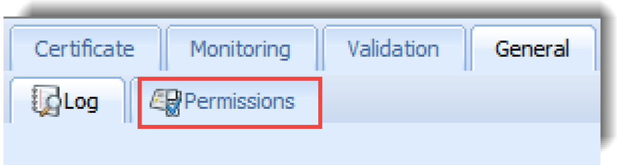
Associate	If you have Write permissions to a Certificate object and both Associate and View permissions to the application(s) where the certificate is installed, you can perform the following functions in the Certificate object's Certificate Associations page: • Associate or disassociate the application with the certificate • Push the certificate and private key to that application • Retry the certificate installation • Enable or disable the processing of certificates on the application. When you disable processing, Trust Protection Platform does not attempt to install, 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
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. This permission is relevant only to Policy, Certificate, and Private Key Credential objects.
Manage Permissions	Grant other user or group Identities permissions to the current object or subordinate objects. In the Web Administration Console, this permission is called Admin.

3.2.2 Assigning Object Permissions to User and Group Identities

In Trust Protection Platform, all administrative permissions are managed at the object level. Every encryption system object—folders, Credentials, Workflows, CAs, Devices, Applications, Certificates, Notifications, Channels, Logging Applications, Discoveries, and Discovery Surveys—has a **Permissions** tab. From an object's **Permissions** tab, you select the users or groups to whom you want to give permissions to the current object (and its subordinate objects). And then you select which permissions you want those users or groups to have. Because permissions flow down the tree, assigned permissions are also inherited by subordinate objects.

To assign permissions to an object in the Web Administration Console

1. Log in to the Trust Protection Platform Web Administration Console.
2. Select the object you want to grant permissions to.
3. Click the **General** > **Permissions** tab.



4. Click **Add.**
5. Select a User or Group Identity, then click **Select**.
6. Select the permissions you want the User or Group Identity to have, then click **Apply/Save**.

3.2.3 Viewing User Entitlements

You can view the objects to which a user has been granted explicit permissions by viewing the Entitlements tab in a User object. This tab provides a convenient, centralized view of a user or group object’s permissions assignments. Objects to which a user or group has inherited permissions do not display on the Permissions tab.

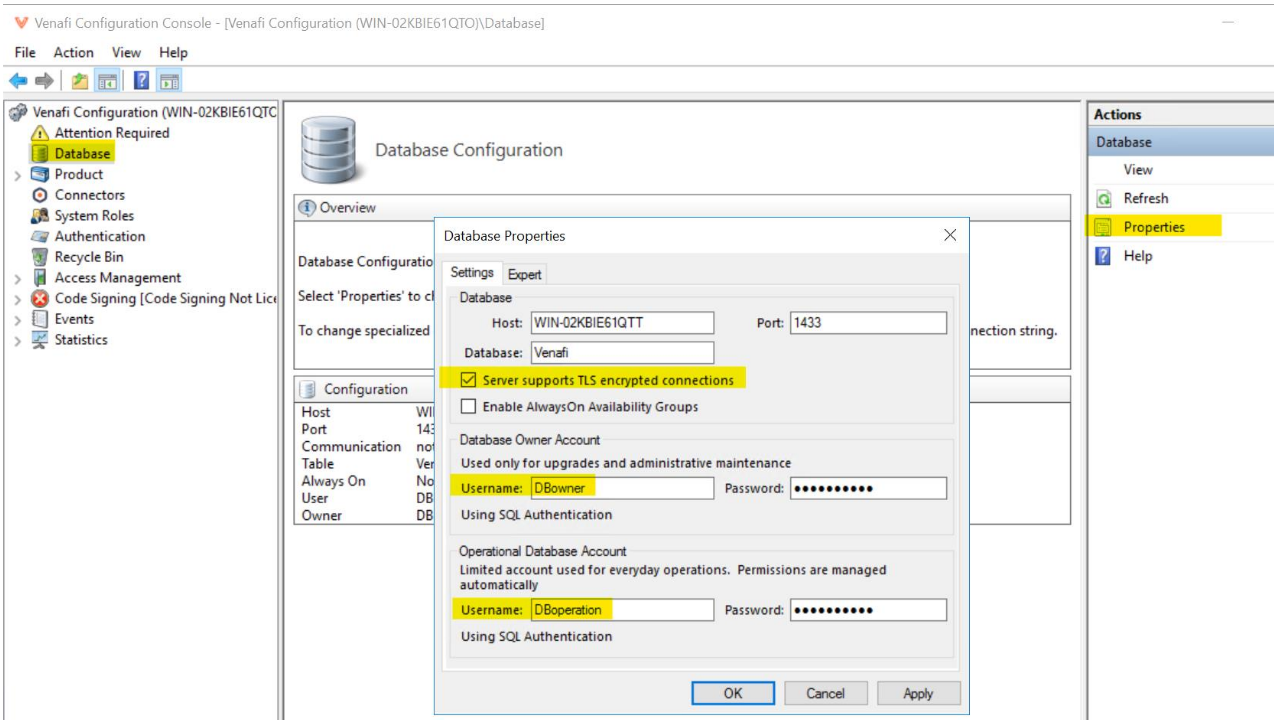
3.3 Secure Database configuration

The TOE supports a local database running on the same host platform or a remote database. Typically, the database is installed on the same host platform. In this case the Host name for the database should be same as the local platform host name.

For a remote database, it should be on the same local area network as the TOE platform. The Host name for the database should be same as the remote platform host name. The remote platform and the database should be configured to support TLS v1.2. The TOE should also be configured to communicate with the remote database securely using TLS. To enable TLS encryption on the TOE using Venafi Configuration Console:

- Navigate to Database tab > Properties
- Enable by clicking on check box for “Server supports TLS encrypted connections”
- Enter the remote database information and click “Apply”

As shown in the screenshot below:



Database

Host: WIN-02KBIE61QTT Port: 1433

Database: Venafi

☑ Server supports TLS encrypted connections

☐ Enable AlwaysOn Availability Groups

Database Owner Account

Used only for upgrades and administrative maintenance

Username: DBowner Password: ••••••••••

Using SQL Authentication

Operational Database Account

Limited account used for everyday operations. Permissions are managed automatically

Username: DBoperation Password: ••••••••••

Using SQL Authentication

4 Testing

4.1 SSH Connectivity

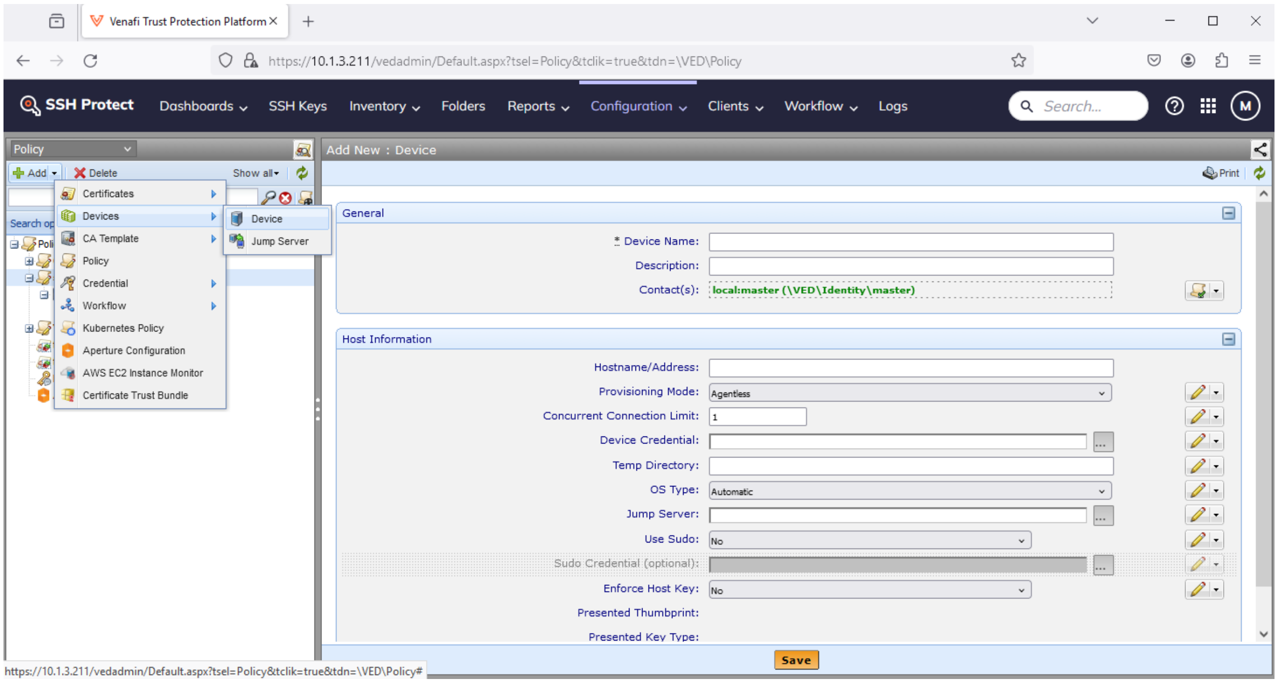
SSH Protect functionality provides visibility, intelligence and automation for your SSH machine identity management. SSH Protect uses outbound SSH communications to manage hosts for:

- Agentless Discovery of User Private Keys, Server Private Keys, Authorized Key files, and Known Host files
- Agentless rotation of User and Server Private Keys and updating the authorized key and known host files
- Agentless installation and rotation of SSH Certificates

NOTE: The Common Criteria evaluation was limited to the secure communication channel with the managed host over SSH. The functionality mentioned above is part of the unevaluated functionality.

To add a managed host:

1. Select SSH Protect from 3x3 square near top right of Aperture interface.
2. Select Policy tree.
3. Click on Add under Policy dropdown.
4. Select Devices > Device



https://10.1.3.211/vedadmin/Default.aspx?tsel=Policy&tclik=true&tdn=\VED\Policy

Add New : Device

General

* Device Name:
Description:
Contact(s): local:master (\VED\Identity\master)

Host Information

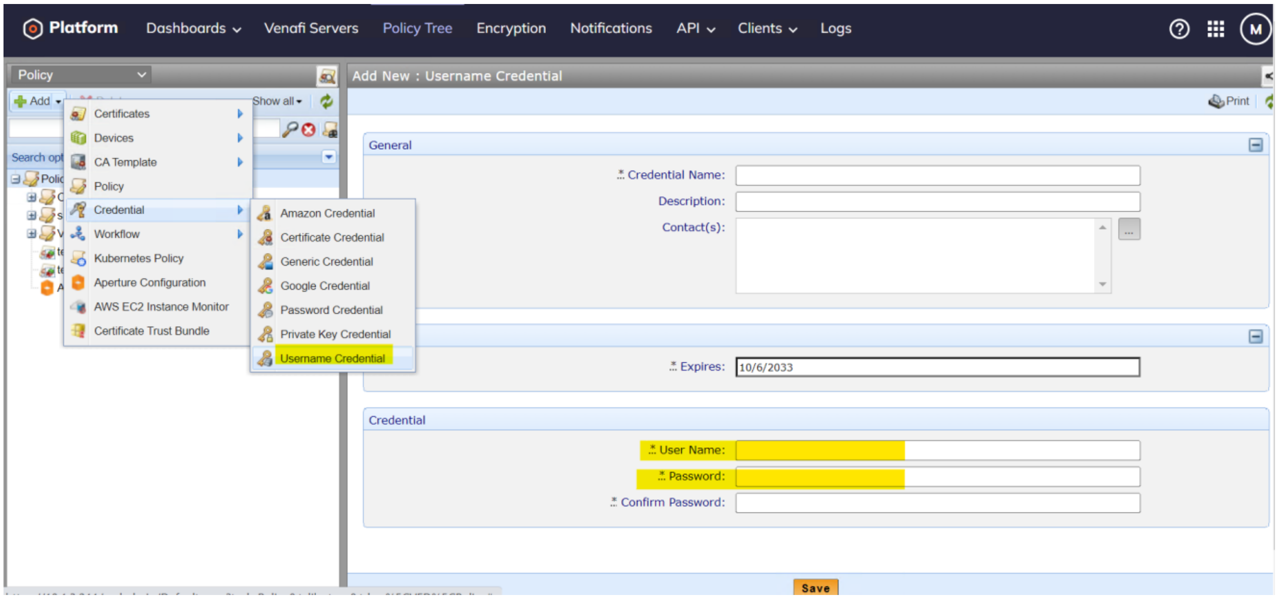
Hostname/Address:
Provisioning Mode: Agentless
Concurrent Connection Limit: 1
Device Credential:
Temp Directory:
OS Type: Automatic
Jump Server:
Use Sudo: No
Sudo Credential (optional):
Enforce Host Key: No
Presented Thumbprint:
Presented Key Type:

https://10.1.3.211/vedadmin/Default.aspx?tsel=Policy&tclik=true&tdn=\VED\Policy#

The TOE supports password based authentication and public key based authentication. Configuration steps are mentioned below.

For password based-authentication the user must configure the credentials from the Web console(Aperture):
1. Select Platform from 3x3 square near top right of Aperture interface.
2. Select Policy tree.

3. Click on Add under Policy dropdown.



Add New : Username Credential

General

Credential Name:

Description:

Contact(s):

Expires: 10/6/2033

Credential

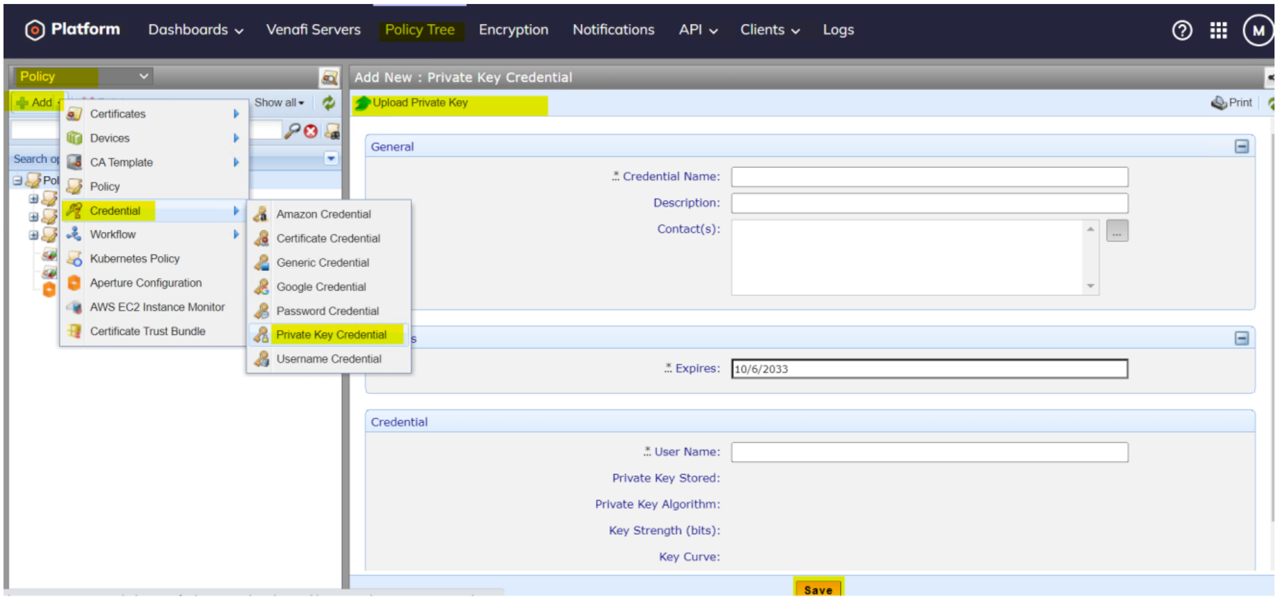
User Name:

Password:

Confirm Password:

For Public key based authentication, the user must upload the private key on the Web console(Aperture)

1. Select Platform from 3x3 square near top right of Aperture interface.
2. Select Policy tree.
3. Click on Add under Policy dropdown.
4. Select Private Key Credential under credential tab.
5. Priavte key can be uploaded by accessing the “Upload Private key” tab.



Add New : Private Key Credential

General

Credential Name:

Description:

Contact(s):

Expires: 10/6/2033

Credential

User Name:

Private Key Stored:

Private Key Algorithm:

Key Strength (bits):

Key Curve:

Note: The following algorithms are not User configurable.

The TOE supports the use of following encryption algorithms:
#1 aes128-ctr,
#2 aes256-ctr,

#3 aes128-cbc, and
#4 aes256-cbc.

The TOE supports the use of following public key algorithms:
#1 ssh-rsa (RFC 4253),
#2 rsa-sha2-256 (RFC 8332),
#3 rsa-sha2-512 (RFC 8332),
#4 ecdsa-sha2-nistp256 (RFC 5656),
#5 ecdsa-sha2-nistp384 (RFC 5656),
#6 ecdsa-sha2-nistp521 (RFC 5656), and
#7 ssh-ed25519 (RFC 8709).

The TOE supports the use of following MAC algorithms (data integrity):
#1 hmac-sha2-256, and
#2 hmac-sha2-512.

The TOE supports the use of following Key Exchange method:
#1 diffie-hellman-group14-sha256 (RFC 8268),
#2 diffie-hellman-group16-sha512 (RFC 8268),
#3 diffie-hellman-group18-sha512 (RFC 8268),
#4 ecdh-sha2-nistp256 (RFC 5656),
#5 ecdh-sha2-nistp384 (RFC 5656),
#6 ecdh-sha2-nistp521 (RFC 5656), and
#7 curve25519-sha256 (RFC 8731).

Note:

- SSH session rekey limits are not User configurable.
- Through .Net the TOE is able to call the Windows cryptographic modules.
- TOE is supporting both RSA and ECDSA for SSH, however, the TOE is only supporting RSA for TLS.

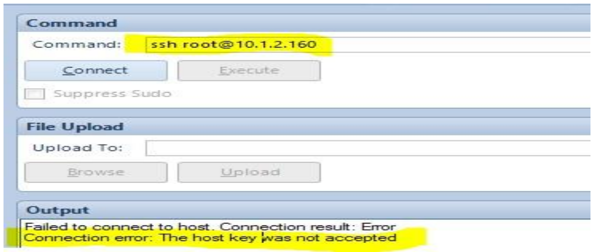
4.2 Adding/Trusting an SSH Server Hostkey to the TOE:

Note: The following algorithms are not User configurable.

The TOE supports the use of following public key algorithms to authenticate its peer (SSH server) host:

- ssh-rsa (RFC 4253)
- rsa-sha2-256 (RFC 8332)
- rsa-sha2-512 (RFC 8332)
- ecdsa-sha2-nistp256 (RFC 5656)
- ecdsa-sha2-nistp384 (RFC 5656)
- ecdsa-sha2-nistp521 (RFC 5656)
- ssh-ed25519 (RFC 8709)

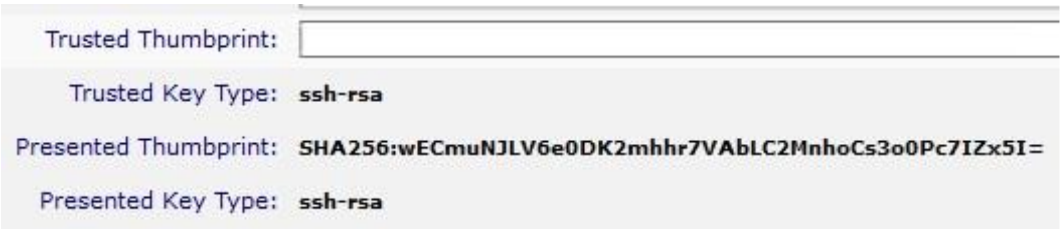
#1 Initiate an SSH connection from TOE to the SSH Server.
#2 The TOE rejects the SSH Server fingerprint on its first encounter as shown below.



Command: ssh root@10.1.2.160

```
Failed to connect to host. Connection result: Error
Connection error: The host key was not accepted
```

#3 By default, the TOE does not trust the presented thumbprint as shown below.



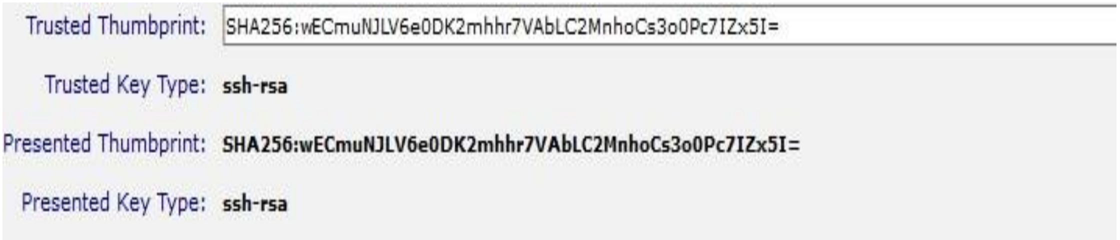
Trusted Thumbprint:

Trusted Key Type: ssh-rsa

Presented Thumbprint: SHA256:wECmuNJLV6e0DK2mhhr7VAbLC2MnhoCs3o0Pc7IZx5I=

Presented Key Type: ssh-rsa

#4 Manually Add the Presented thumbprint to Trusted thumbprint as below:



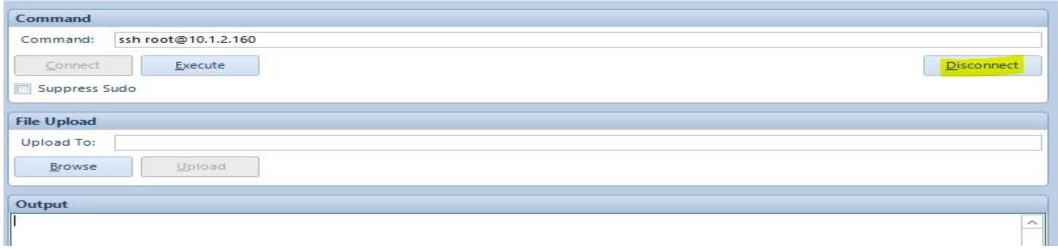
Trusted Thumbprint: SHA256:wECmuNJLV6e0DK2mhhr7VAbLC2MnhoCs3o0Pc7IZx5I=

Trusted Key Type: ssh-rsa

Presented Thumbprint: SHA256:wECmuNJLV6e0DK2mhhr7VAbLC2MnhoCs3o0Pc7IZx5I=

Presented Key Type: ssh-rsa

#4 Initiate an SSH connection from TOE to the SSH Server.
#5 The TOE now successfully connects to the SSH Server as shown below.



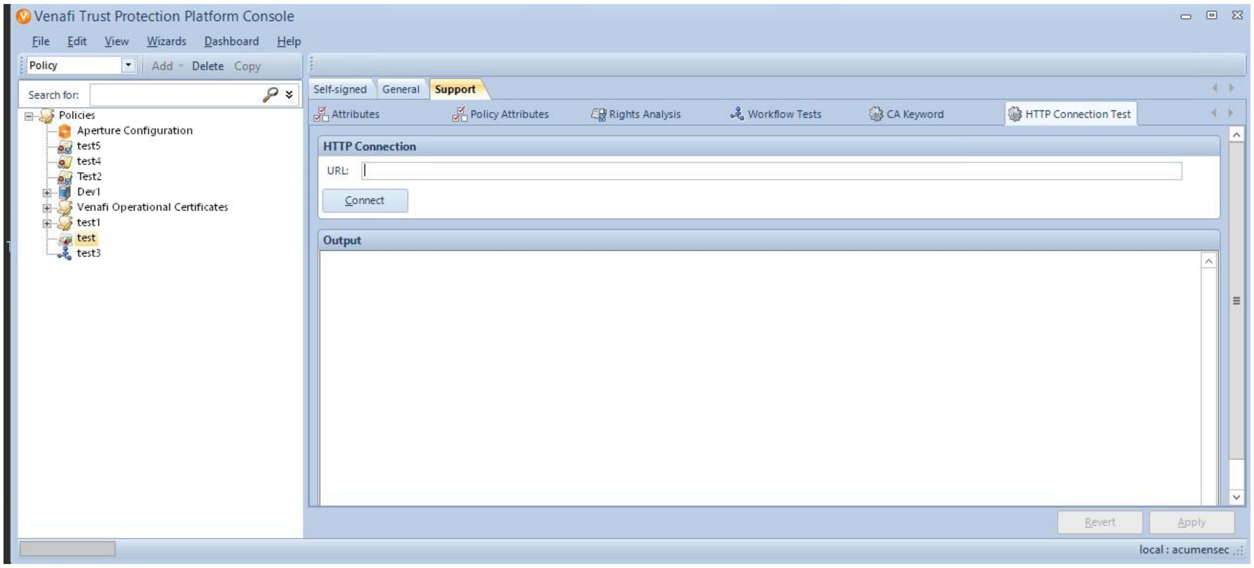
Command: ssh root@10.1.2.160

4.3 TLS Connectivity

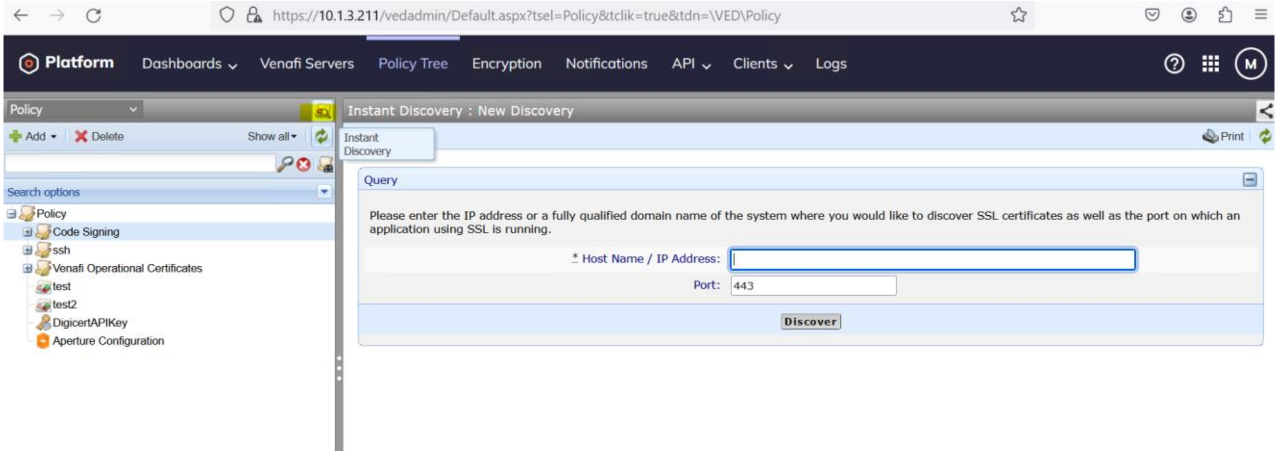
The TOE leverages Microsoft's IIS to provide web services for incoming User or Admin authentication attempts to access the web console. The TLS protocol is provided by the underlying platform. The TOE uses .NET to invoke the platform's TLS functionality.

The product uses TLS to connect to the remote database and to perform discovery services. Please refer to Section 3.3 on instructions to configure the TOE to connect with a remote database over TLS.

Before performing Discovery services, TOE's TLS functionality should be tested using the HTTP Connection Test functionality. Under the Support tab go to the HTTP Connection Test tab. The URL of the connection endpoint is used as the reference identifier.



To perform “Discovery Services”:
1. Select Platform from 3x3 square near top right of Aperture interface
2. Click on small magnifying glass, instant discovery option
3. Enter the hostname or IP address and click on discovery to perform discovery



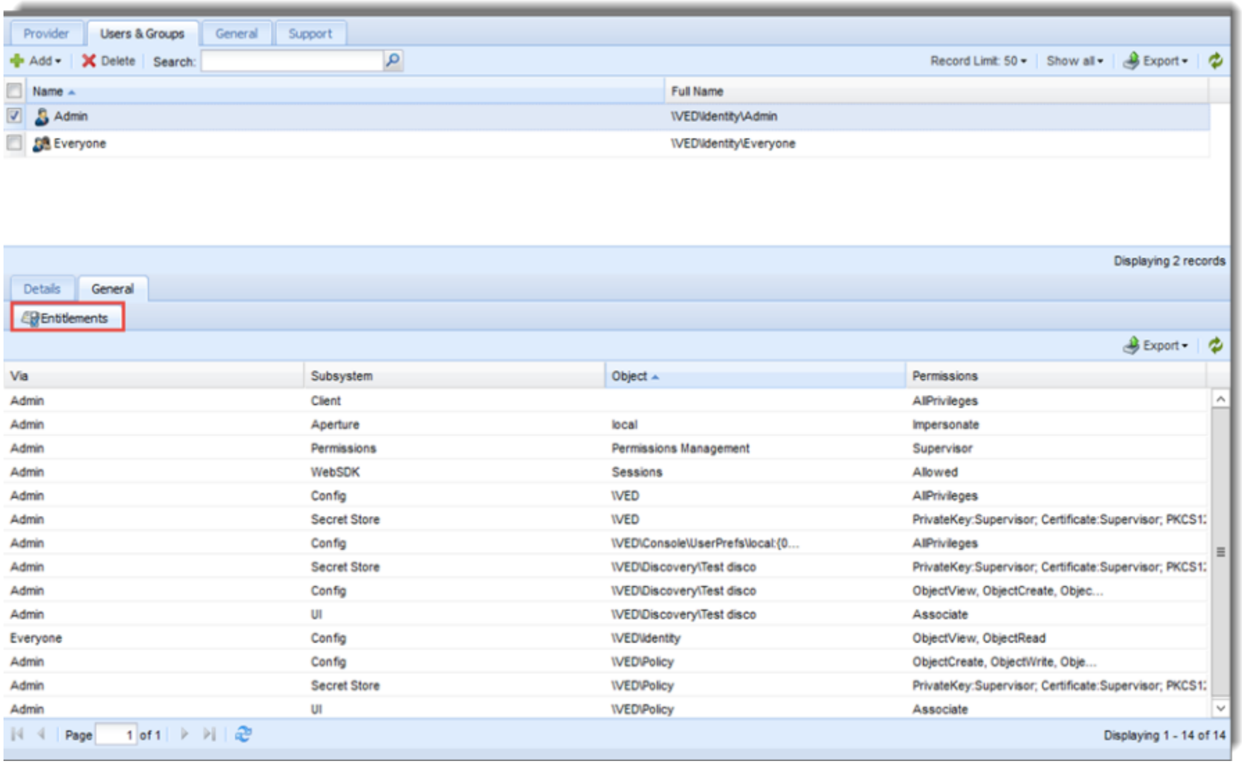
Please enter the IP address or a fully qualified domain name of the system where you would like to discover SSL certificates as well as the port on which an application using SSL is running.

* Host Name / IP Address:

Port: 443

Entitlements in the Web Entitlements Console

In the Web Administration Console, the user entitlements are listed on a user object’s General tab.



	Name	Full Name
☑	Admin	\VED\Identity\Admin
□	Everyone	\VED\Identity\Everyone

Displaying 2 records

Via	Subsystem	Object	Permissions
Admin	Client		AllPrivileges
Admin	Aperture	local	Impersonate
Admin	Permissions	Permissions Management	Supervisor
Admin	WebSDK	Sessions	Allowed
Admin	Config	\VED	AllPrivileges
Admin	Secret Store	\VED	PrivateKey:Supervisor; Certificate:Supervisor; PKCS1:
Admin	Config	\VED\Console\UserPrefs\local:{0...	AllPrivileges
Admin	Secret Store	\VED\Discovery\Test disco	PrivateKey:Supervisor; Certificate:Supervisor; PKCS1:
Admin	Config	\VED\Discovery\Test disco	ObjectView, ObjectCreate, Objec...
Admin	UI	\VED\Discovery\Test disco	Associate
Everyone	Config	\VED\Identity	ObjectView, ObjectRead
Admin	Config	\VED\Policy	ObjectCreate, ObjectWrite, Obje...
Admin	Secret Store	\VED\Policy	PrivateKey:Supervisor; Certificate:Supervisor; PKCS1:
Admin	UI	\VED\Policy	Associate

Displaying 1 - 14 of 14

4.4 X509 Certificate Validation and Configuring CA Server

4.4.1 X509 Certificate Validation

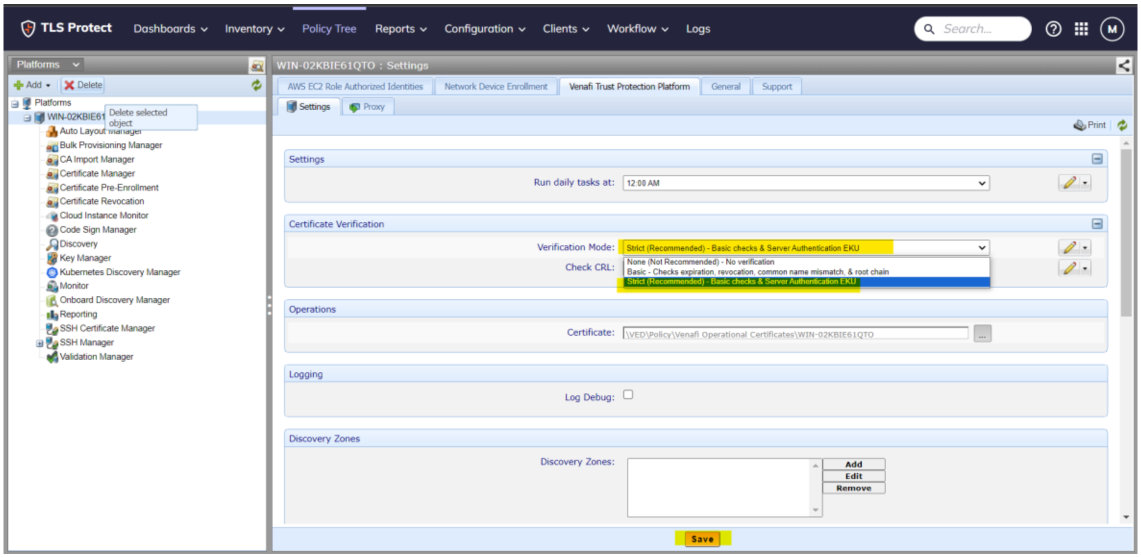
The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. All certificate validation is performed by invoking the underlying Windows platform, and certificates are stored in the Windows certificate store. The TOE supports a chain length four or greater.

Certificate validation paths must terminate with a trusted CA certificate that contains the basicConstraints extension and a CA flag that is set to TRUE. ExtendedKeyUsage field validation is also performed.

Administrator should configure the platform settings verification mode to strict for verification of certificates. To enable Verification of certificates:

1. Select Platform from 3x3 square near top right of Aperture interface.
2. Select Venafi Servers.
3. Selecat a server under Platforms on which the CRL verification should be enabled.
4. Click on Settings Tab.
5. Under Certificate Verification > Verification Mode, select “Strict”.

6. Click Save.



WIN-02KBIE61QTO : Settings

Settings

Run daily tasks at: 12:00 AM

Certificate Verification

Verification Mode: Strict (Recommended) - Basic checks & Server Authentication EKU

- None (Not Recommended) - No verification
- Basic - Checks expiration, revocation, common name mismatch, & root chain
- Strict (Recommended) - Basic checks & Server Authentication EKU

Check CRL:

Operations

Certificate: \VED\Policy\Venafi Operational Certificates\WIN-02KBIE61QTO

Logging

Log Debug: □

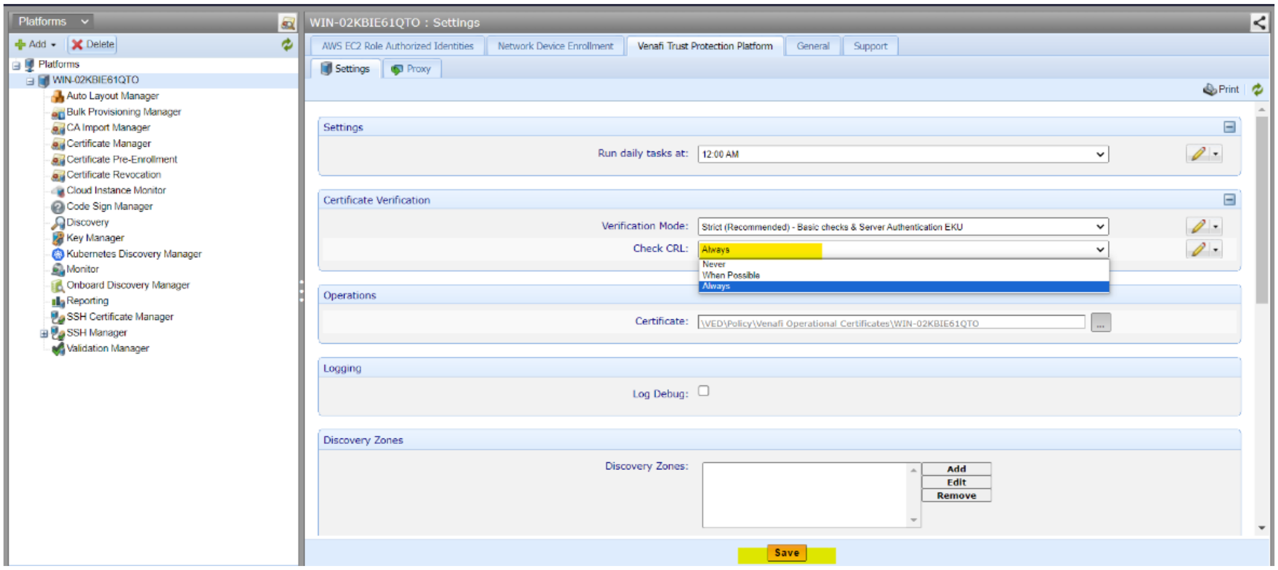
Discovery Zones

Discovery Zones:

4.4.1 Configuring CA Server

The TOE supports validation of the revocation status of the certificate using CRL. CRLs are configurable and should be used for certificate revocation. The TOE can be configured for CRL checking and validation as follows:

7. Select Platform from 3x3 square near top right of Aperture interface.
8. Select Venafi Servers.
9. Selecat a server under Platforms on which the CRL verification should be enabled.
10. Click on Settings Tab.
11. Under Certificate Verification > Check CRL, select “Always”.
12. Click Save.



WIN-02KBIE61QTO : Settings

Settings

Run daily tasks at: 12:00 AM

Certificate Verification

Verification Mode: Strict (Recommended) - Basic checks & Server Authentication EKU

Check CRL: Always

- Never
- When Possible
- Always

Operations

Certificate: \VED\Policy\Venafi Operational Certificates\WIN-02KBIE61QTO

Logging

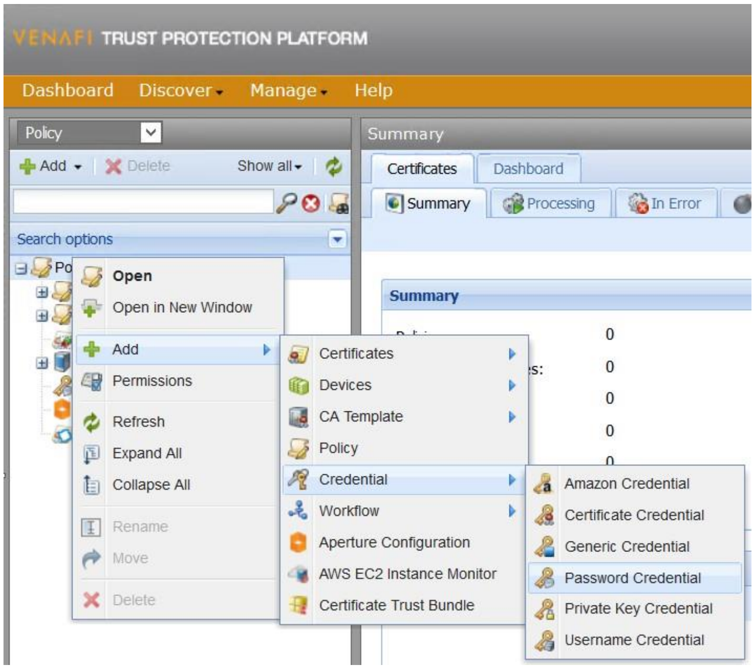
Log Debug: □

Discovery Zones

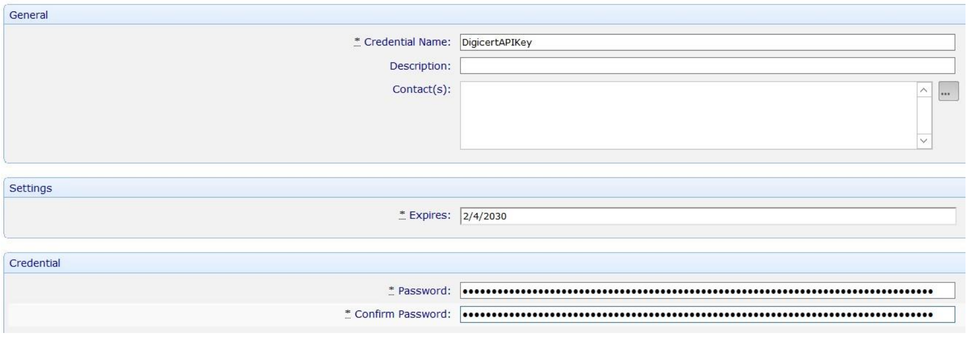
Discovery Zones:

Additionally, external CA servers can be configured as below:

#1 Policy -> Add->Credential->Password Credential.



#2 Enter password (e.g 12345678910123456789101234567891O).



General

* Credential Name:	DigicertAPIKey
Description:	
Contact(s):	

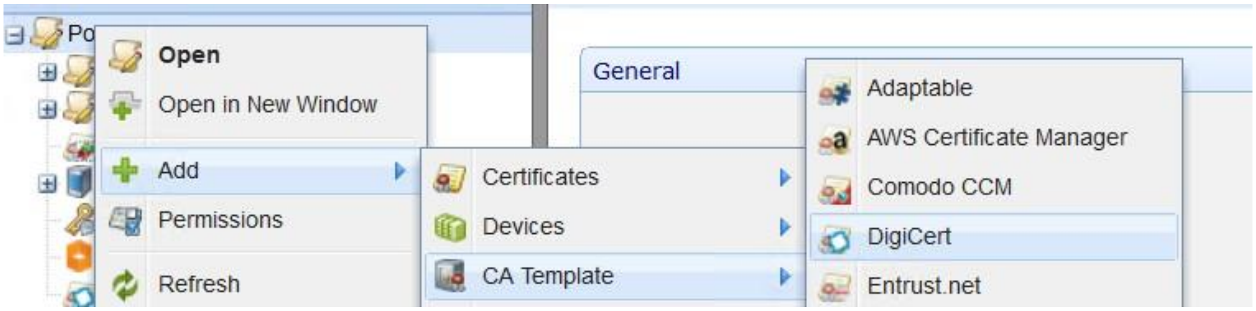
Settings

* Expires:	2/4/2030

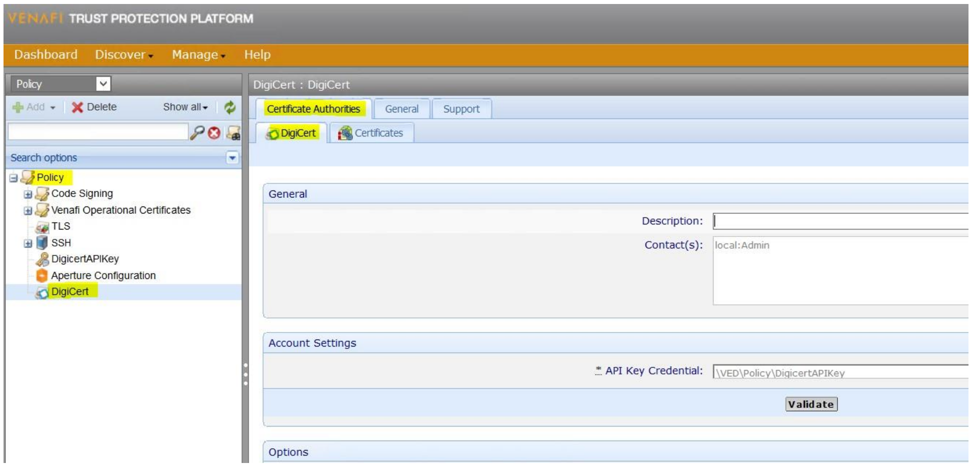
Credential

* Password:	••
* Confirm Password:	••

#3 Policy->Add->CA Template->DigiCert.



#4 CA Server will now be configured.



Description:

Contact(s): local:Admin

* API Key Credential: \VED\Policy\DigicertAPIKey

4.5 TOE Access to Platform Resources

Network connectivity is the only platform hardware resource accessed by the TOE. The TOE leverages Microsoft IIS webserver for User or Admin authentication over web-based console. The TOE also communicates with an external database, managed hosts, CA servers, and to perform discovery services.

System logs are the only sensitive information repository accessed by the TOE. The TOE accesses system logs (i.e. Windows Event log) for the purpose of writing events to the logs.

4.6 Management Functions

TOE administrators can enable and disable the following:

4.6.1 Transmission of any application state information

The TOE administrator can enable and disable Stack Traces as described below:

- Stack Traces: Navigate to C:\Program Files\Venafi\Web\Aperture\API\web.conf file. ○ Change the "showStackTrace" value from 0 to 1. This enables Stack Traces for the TOE.

4.6.2 Debug level logging

1. Open Venafi Trust Protection Platform

2. Select Platforms from the Drop-Down menu

3. Select the Windows machine on which the Venafi Trust Protection Platform is installed.

4. Enable/Disable Logging

Alternatively, this ca also be achieved as follows:

1. Open Venafi Configuration Console.

2. Select Product.

3. Click on Logging

4. Enable/Disable Logging via the Actions pane

4.6.3 Services module

1. The services modules can be Enabled or Disabled by selecting Service Module (e.g. Certificate Manager, SSH Manager) from the Venafi Trust Protection Platform.
2. Click on Platforms from the Drop-Down Menu
3. Select Service Module of your choice.
4. Check or Uncheck Disabled.

4.6.4 Web applications

After installing the Venafi Trust Protection Platform, the Admin is given the option to enable/disable various web applications.

Once created, these applications can be modified by running the Venafi Control Center.

1. Open the Venafi Trust Protection Platform installation directory (e.g. C:\Program Files\Venafi\Platform)
2. Start Venafi Configuration Console
3. Expand Product list from the menu.
4. Select web application of your choice.
5. Start/Stop/Restart/Refresh the appropriate web application by clicking the corresponding buttons available.

5 Upgrade Bug Fix

5.1 Symptom

After TPP v23.1.0 install VCC launches without issue. When closing VCC and launching a second time, the upgrade experience occurs.

5.2 Resolution

1. Open Notepad.exe as Administrator.
2. Select File > Open and find the "231.xml" file in your Venafi install directory.
   - NOTE: You may need change the file type from "Text Documents (*.txt)" to "All Files (*.*)" for xml files to be visible
   - Default path: C:\Program Files\Venafi\Schema\231.xml
3. Search the text file for “23010001756” and replace all occurrences with "23010001776"
4. Save the file
5. Open CMD as administrator and run the following commands. Replace the example paths with your Venafi install directory if it differs. Replace the username "admin" with your Master Admin username:

```
cd "C:\Program Files\Venafi\Platform"
schematool admin "C:\Program Files\Venafi\Schema\231.xml"
```

Instructions for using SchemaTool:
https://support.venafi.com/hc/en-us/articles/215911887-Info-Using-Schematool [support.venafi.com]
The final schematool step applies the changes made to the 231.xml file to the schema.

6 TOE Patches

To install patches,

stop all Venafi services on the TOE, replace the dll, and then restart services.

Run the following three commands in the command line to stop Venafi services.

```
sc stop venafilogserver

sc stop ved

sc stop venafiwcfhost
```

Then, copy the patched DLL file into the
\Windows\Microsoft.NET\assembly\GAC_MSIL\Maverick.NET\v4.0_2.0.3.0__a87e673e9ecb6e8e\
directory.

Afterwards, run the following four commands to restart services, as well as the Web host service.

```
sc start venafilogserver

sc start ved

sc start venafiwcfhost

iisreset
```

7 TOE Updates

The product has functionality built in to inform administrators when a patch for the version in use is released, or when a new version is released. This functionality will not work if there is no external network access.

To Check for Updates:

1. Login to the TOE via Web-based Console.
2. Navigate to My Account.
3. Click About. This shown the current version of the TOE.
4. Check if there is any notification for an upgrade or patch being available.
   a. Absence of any notification indicates that no updates are available.
   b. If there is a notification for a patch or a new release, please follow the instructions in Section 8 to download the update.
5. Click on Upgrade Status to check if the upgrade was complete.

To query the current version of the TOE from Trust Protection Platform:

a. Open Venafi Trust Protection Platform.

b. Click on Help.

c. Click on About Console.

d. Check the Version of the TOE.

To Upgrade Trust Protection Platform:

1. Back up the Trust Protection Platform database.
2. Stop IIS.
3. Stop all Trust Protection Platform services.
   a. Stop the Trust Protection Platform service.
   b. Stop the Venafi UniCERT Interface service, if present.
   c. Stop the Venafi Log Server service.
4. Close all Venafi-related Windows applications. For example, close any browsers that are logged into User Portal, Aperture, or the Web Administration console.
5. Repeat steps 2 and 3 on all Trust Protection Platform servers to ensure all Venafi-related services are stopped prior to continuing with step 6.
6. Unzip "Venafi Trust Protection Platform 23.1.1.zip". Run the VenafiTPPInstall-23.1.1.msi as an Administrator (e.g. launch the Command Prompt with "Run as Administrator" and then launch the installation MSI file). Complete the on-screen walkthroughs, per your environment's requirements.

   Note:
   - All binaries are signed using signtool.exe, which is a .Net framework tool for digital file signatures, to ensure they come from the authorized source – via download https://download.venafi.com/. Users must have a username and password to login to download the binaries.
7. Query the Trust Protection Platform:

   a. Open Venafi Trust Protection Platform

   b. Click on Help

   c. Click on About Console

   d. Check the Version and confirm update successful.

8 Secure Acceptance of TOE

To download the latest version of Trust Protection Platform:

1. Navigate to https://download.venafi.com and log in with your Venafi Customer Support credentials. If you don't have an account, you can register at

https://success.venafi.com/signin/register. If your account does not have access to the downloads site, and you think it should, please contact Venafi Customer Support.

2. Expand the Trust Protection Platform group, then expand Current.
3. In each folder inside the Current folder, download the zip file.
4. Store the zip file(s) in your software repository, if applicable.
5. Copy the installer (and any patch) to each of the Venafi servers.

Published Hash verification:

To obtain Published hash, open the zip file downloaded from https://download.venafi.com.

The zip file should contain the Sha256 Checksum file:
“CheckSums.sha256”.

9 Security Functions provided by the TOE

The TOE provides the security functionality required by [SWAPP].

9.1 Cryptographic Support

The TOE relies on underlying cryptographic functionality provided by the platform for all of its cryptographic operations, as allowed by the [SWAPP].

9.2 Security Management

The TOE does not come with any default credentials. Upon installation it will randomly generate a self-signed certificate, and AES 256 symmetric key and a GUID for the base configuration of the system. No data is stored by the application on the platform file system.

9.3 Privacy

The TOE does not store or transmit anything that could be considered Personally Identifiable Information (PII).

9.4 User Data Protection

The TOE relies on the platform to securely store the following:

- DSN key
- PKCS12 key
- PKCS8 (private key)
- Usernames
- Passwords
- Customer application credentials

The Windows Registry is used for storage of the TOE’s symmetric key. An AES 256 key is used for the encryption and decryption of secrets. It is protected by the Windows Data Protection API (DPAPI).
No additional sensitive data is stored by the TOE.

9.5 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE never allocates memory with both write and execute permission. The TOE is designed to operate in an environment in which the following security techniques are in effect:

- Data execution prevention,
- Mandatory address space layout randomization (no memory map to an explicit address),
- Structured exception handler overwrite protection,
- Export address table access filtering, and
- Anti-Return Oriented Programming.

This allows the TOE to operate in an environment in which the Enhanced Mitigation Experience Toolkit is also running. During compilation, the TOE is built with several flags enabled that check for engineering flaws. The TOE is built with the /GS flag enabled. This reduces the possibilities of stack-based buffer overflows in the product.

9.6 Trusted Path/Channels

TLS and SSH are used to protect all data transmitted to and from the TOE.

9.7 Unevaluated Functionality

The following functionality is outside the scope of the evaluation:

- Providing visibility, threat intelligence, policy enforcement, and incident response for certificate-related outages and key compromises
- Integration with Venafi products and third-party applications – the evaluation is limited to secure communication channels
- Visibility into their key and certificate inventory, certificate reputation
- Issuance and renewal of certificates
- Policy enforcement
- Workflows
- Remediation of key and certificate misuse