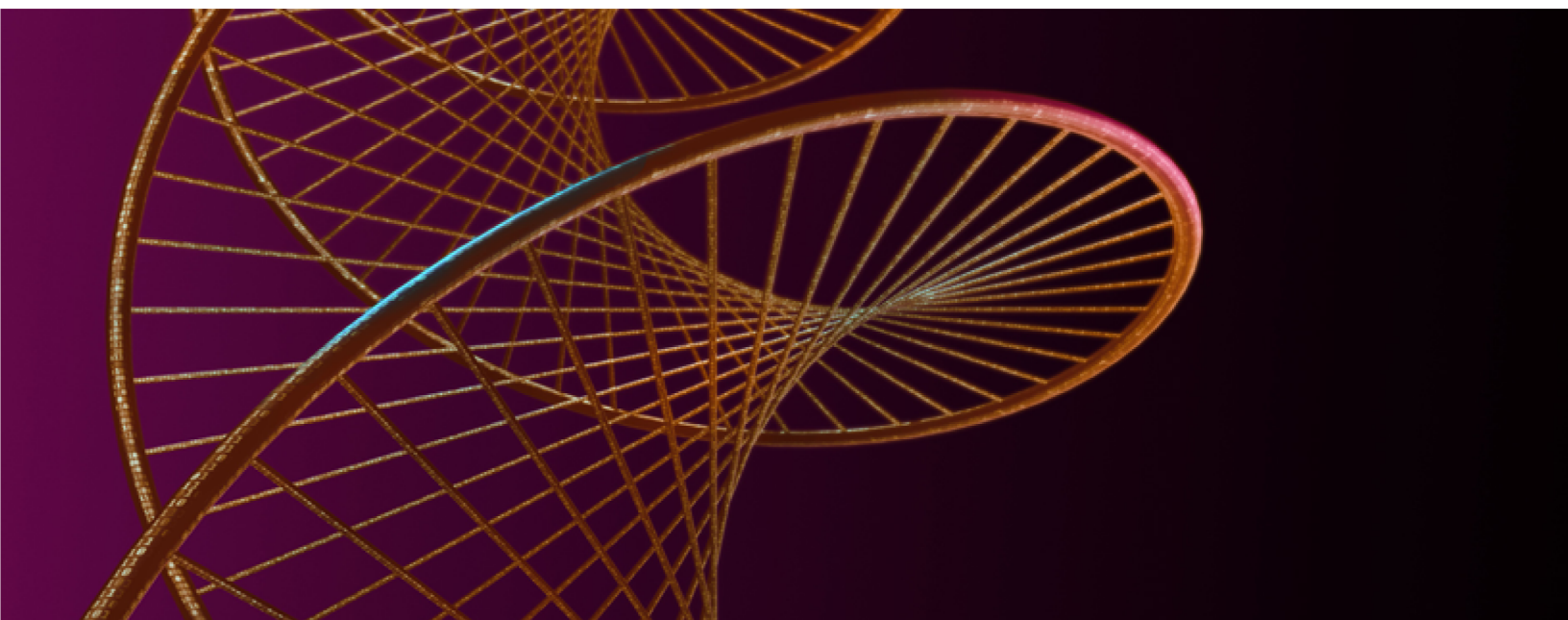


Venafi Trust Protection Platform 25.1

Installation and Upgrade Guide



Legal Notices

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

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

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

Online Documentation

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

Feedback - We love hearing from you

We welcome your feedback on our documentation. If you have something you'd like to share, or a way we could improve, please send the following information to documentationfeedback@venafi.com: [1] The name of the PDF guide (Installation and Upgrade 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>

About this guide	6
Audience	6
Chapter 1: System requirements for Venafi components	7
Venafi Trust Protection Platform components	7
Common requirements (on-premises or cloud-based databases)	14
Network access requirements	26
Server Agent	28
Venafi Certificate Authority Drivers	30
Provisioning (Certificate Installation) Drivers	31
Supported browsers and supported vendors, products, and versions	33
Chapter 2: Installing Trust Protection Platform	39
Preparing your environment for the Venafi Platform	41
Reviewing system requirements before installation	42
Determining the number of Windows servers needed	42
Deploy and configure the Windows servers	42
Network connectivity requirements	48
Database Encryption	51
Installation preparation worksheet	53
Preparing the database server	59
Which edition of Microsoft SQL Server should I use?	59
Setting up your Microsoft SQL database server	60
AlwaysOn high-availability disaster recovery solution	63

Windows permissions for database service accounts	64
Using Group Managed Service Accounts (gMSAs)	65
Installing and Configuring Venafi servers	66
Downloading the latest version of Venafi Trust Protection Platform	67
Installing using the Venafi Configuration Console wizard	67
Trust Protection Platform components	80
Command line installation and configuration	87
Downloading the latest version of Venafi Trust Protection Platform	88
Creating and using answer files	89
Install the MSI file from the command line	96
Configure the platform using a script through the command line	97
Using the TppConfiguration command line tool	99
Run script and review response codes	106
Database Encryption	108
Automatic credential rotation options	110
Post-installation procedures	113
Starting Venafi Trust Protection Platform services	113
Securing Trust Protection Platform's web servers	114
Backing up the software encryption key	114
Adding another server to the Trust Protection Platform network	116
Configuring general SMTP options for outbound email notifications using Policy Tree	117
Chapter 3: Upgrading Venafi Platform 25.1.x	119
Preparing to upgrade to 25.1	119
About rolling upgrades	121
Review the release documentation	123
Trust Protection Platform upgrade options	124
Upgrade steps	126

In place rolling upgrade	127
Replace rolling upgrades	130
Offline upgrade	134
Upgrade using the command line	138
Upgrade status icon and page	139
 Chapter 4: Updating the latest patch	 141
 Chapter 5: Uninstalling Venafi Trust Protection Platform	 142
 Chapter 6: Disaster recovery operations	 144
High availability disaster recovery	145
Fault tolerance	145
High availability disaster recovery	145
Trust Protection Platform standby mode	145
Before you begin disaster recovery procedures	146
How to recover a lost Trust Protection Platform server	146
How to recover a lost Trust Protection Platform database (Microsoft SQL)	147
How to recover a broken HSM connection	147
 Appendix A: Contact information	 150
Venafi Corporate Office	150
Support Services	150
Venafi Customer Support	150

About this guide

Welcome to Venafi Trust Protection Platform™, a tool that enables organizations to rapidly develop an accurate certificate inventory and identify security and operational risks. Additionally, 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, Trust Protection Platform helps eliminate data breaches, security audit failures and unplanned system outages.

The *Venafi Trust Protection Platform Installation Guide* presents the information you need to successfully install Trust Protection Platform. It reviews the requirements and pre-installation procedures such as configuring SSL and ports on a Windows server. The guide then walks you through the installation process and initial database configuration.

Audience

The Venafi Trust Protection Platform installation guide is written for server hardware and software administrators who are responsible for managing servers, including the installation and upgrade of systems on those servers.

1

System requirements for Venafi components

Before installing and using any Venafi product, carefully review Venafi's supported operating system and hardware configurations.

Also, review any additional or special requirements specified in the documentation provided with each product.

NOTE To view the system requirements for previous releases, visit: <https://docs.venafi.com/>.

Venafi Trust Protection Platform components

Supported Software and Hardware Configurations

Hardware requirements

Feature	Requirement
Processor	4 processing cores
Memory	16 GB RAM
Disk Space (for the Trust Protection Platform application)	5 GB

Feature	Requirement
	The Trust Protection Platform application can be installed on a secondary partition.

Number of Trust Protection Platform servers needed

Feature	Requirement
Number of Venafi servers (Up to 50K active certificates, 1K SSH servers, and 175 code signing requests per second*)	2 total (assuming all in-use features are enabled on both servers)
Number of Venafi servers (Up to 250K or more active certificates and 5K SSH servers)	6 total 2 dedicated Logging event processing servers 2 web services servers 2 back end processing servers
Number of Venafi servers (Up to 1M or more active certificates and 20K SSH servers)	Implementations of this size are professionally designed by Venafi according to the customer's needs.
Server Agents doing SSH work	2 additional Venafi servers for every 20,000 SSH servers being managed

Feature	Requirement
Server Agents doing certificate work	2 additional Venafi servers for every 40,000 servers being managed

Network latency to database	For best performance results, you should minimize the network latency between the database server and the Venafi Platform servers.
-----------------------------	--

For comparison, we compared the following at various latency levels:

- Time required to renew a certificate
- Number of code signing requests per second.

These numbers are from a configuration using two Venafi Platform servers configured with the [minimum hardware requirements](#). They represent a mix of ECC and RSA keys and were derived using the CodeSign Protect HSM REST API. Results may vary if you are using other mechanisms.

WAN Delay (in milliseconds)	Time to renew 1 certificate	Code signing requests per second
0	around 2 seconds	around 190
15	around 7 seconds	around 99
30	around 15 seconds	around 48
60	around 30 seconds	around 24
120	around 60 seconds	around 12

While these speeds are *not* guaranteed, they *are* illustrative of the significant impact latency can have on overall system performance.

Network latency to HSM	For best performance, minimize the latency between your HSM and your Venafi Platform servers.
------------------------	---

These numbers are from a configuration using two Venafi Platform servers configured with the [minimum hardware requirements](#). They represent a mix of ECC and RSA keys and were derived using the CodeSign Protect HSM REST API. Results may vary if you are using other mechanisms.

Feature	Requirement												
	While these speeds are <i>not</i> guaranteed, they <i>are</i> illustrative of the impact latency can have on system performance. Your HSM performance will affect your final result.												
	<table> <tr> <th>WAN Delay (in milliseconds)</th><th>Code signing request per second</th></tr> <tr> <td>1</td><td>around 175</td></tr> <tr> <td>15</td><td>around 85</td></tr> <tr> <td>30</td><td>around 49</td></tr> <tr> <td>60</td><td>around 25</td></tr> <tr> <td>120</td><td>around 15</td></tr> </table>	WAN Delay (in milliseconds)	Code signing request per second	1	around 175	15	around 85	30	around 49	60	around 25	120	around 15
WAN Delay (in milliseconds)	Code signing request per second												
1	around 175												
15	around 85												
30	around 49												
60	around 25												
120	around 15												

* Total number of signing request per second using a variety of ECC and RSA keys on an HSM, and using the HSM REST API to sign.

Server Configuration requirements

Feature	Requirement
Operating Systems	- Microsoft Windows Server 2022 (server with user interface) is <i>supported</i> (and required if you want to use TLS 1.3). - Microsoft Windows Server 2019 (server with user interface) is <i>supported</i>. - Microsoft Windows Server 2016 (server with user interface) is <i>supported</i>. Trust Protection Platform only supports English Language Installation Media from Microsoft. While it does support region setting configurations to ensure that date and times appear correctly, the Windows servers on which you install Trust Protection Platform must be derived from Windows English installation media.

Regarding job scheduling and timezones, there is a potential issue with timezone support on different Windows Server versions. Newer Windows Server versions may have updated timezones that older versions cannot parse correctly. This could lead to scheduling issues. It is recommended to have consistent OS versions across Trust Protection Platform servers.

Multiple servers connected using the same database are referred to as a cluster. To help you understand how your cluster is connected together, and to facilitate communication between servers in the cluster, Venafi Platform provides a feature called Message Bus, which uses an MQTT broker to maintain near-immediate connection between all servers in the cluster. Venafi Platform includes its own MQTT broker which allows the servers in the cluster to communicate in mesh mode. You can also use a separate external MQTT broker to allow your servers to communicate via the MQTT broker (hub-and-spoke mode). For details on how to use Message Bus, see [Message Bus](#).

If you have three or more Venafi servers, some servers may not require the features in the following table, which lists additional server requirements and roles only for those Venafi servers that support inbound web services. For more information, see "[Enable web services on required servers](#)" on [page 43](#).

Feature	Requirement
Web Server Roles (Venafi web services enabled)	Install the following required Microsoft Internet Information (IIS) web server roles: ▪ 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
Windows Server Roles	Microsoft Windows 2022 Server
(Web Server\Application Development\ .NET Extensibility)	▪ ASP.NET 4.8 ▪ ISAPI Extensions ▪ ISAPI Filters

Feature	Requirement
	■ .NET Extensibility 4.8
	Microsoft Windows 2019 Server
	■ ASP.NET 4.6 ■ ISAPI Extensions ■ ISAPI Filters ■ .NET Extensibility 4.6
	Microsoft Windows 2016
	■ ASP.NET 4.5 ■ ISAPI Extensions ■ ISAPI Filters ■ .NET Extensibility 4.5
Microsoft runtime libraries	You need to install both the following Visual C++ Runtime libraries: ■ 32-bit version ■ 64-bit version For more information, see the following from Microsoft: Latest supported Visual C++ Redistributable downloads
Windows service dependencies	The following services should not be disabled: ■ CNG Key Isolation (for elliptic curve key operations)

Feature	Requirement
IIS 7.5 Add-On	Microsoft URL Rewrite Module 2.1
.NET Framework (Venafi web services enabled)	.NET Framework 4.8 is <i>required</i> for all OS versions. Download .NET Framework 4.8 from https://dotnet.microsoft.com/download/dotnet-framework/net48.
Port 80 Binding Requirements	If you are using SCEP (Simple Certificate Enrollment Protocol), you must allow port 80 binding. SCEP will not work without port 80 binding. Additionally, the timestamping service requires port 80. If access to port 80 is blocked, the Time Stamp Service endpoints in CodeSign Protect will not be able to get timestamping data. If you are not using SCEP, and you don't care about access to the Time Stamp Service Endpoints, you can disable access on Port 80.

TIP You can save valuable time in assessing and installing system prerequisites by running the Prereq Check Script and the Base Configuration Utility available at <https://download.venafi.com/>. After signing in, expand **PS Utilities** and download the following:

- Prereq Check Script¹
- Base Configuration Utility²

Supported Databases

Trust Protection Platform requires a database to store system configuration information, archive certificates and private keys, and secure sensitive data.

¹A PowerShell script that rapidly verifies whether or not all Venafi Platform prerequisites are installed already and reports which ones are not. You can even use the optional `Install` parameter to automatically install some missing items and remove the IIS default web site, something typically done manually following installation of the Venafi Platform.

²Download and run this utility to set most of the common post-install checklist requirements automatically, including the creation of best-practice policy tree folders, workflows, notifications, and discovery placement rules.

Common requirements (on-premises or cloud-based databases)

For specifics about setting up a cloud instance using a supported cloud provider, see ["Cloud hosting using Amazon RDS, Azure SQL managed Instance, or Google Cloud SQL"](#) on page 16.

BEST PRACTICE Venafi recommends having enough drive space available on the SQL server to restore an entire copy of the database if required for recovery or troubleshooting. During a critical problem resolution, if the need arises to restore an older copy of the database for comparison or data recovery, it is a best practice to ensure that it is possible to have the current and previous databases available simultaneously.

Feature	Description
Supported platforms	The database should <i>not</i> be installed on the Trust Protection Platform server except in test environments. SQL AlwaysON Availability Groups are supported for Disaster Recovery and High Availability. Unless otherwise specified, all updates, patches, and service packs (SPs) for the Microsoft SQL Server versions (in English only) listed below are supported by Venafi Trust Protection Platform. If an SP is specified below, it represents the minimum SP required for the given SQL version. If you use a cloud server for Trust Protection Platform, you should use it for both the database and the Venafi Platform servers. <i>We do not recommend splitting between a cloud provider and on-prem.</i> Venafi typically releases major software updates every six months. Microsoft releases new SPs and patches for its SQL Server versions regularly. Releases rarely occur at the same time. Venafi recommends that you keep your SQL Server version updated with the latest SPs and patches from Microsoft. Supported: ▪ Microsoft SQL Server 2022 ▪ Microsoft SQL Server 2019 ▪ Microsoft SQL Server 2017 ▪ Microsoft SQL Server 2016 SP2 ▪ Microsoft SQL Server 2014 For more information, see the SQL Server installation guide. IMPORTANT Currently Venafi Platform is only supported on English installations of Microsoft SQL Server.

Feature	Description
Database recovery model requirements	For databases containing Trust Protection Platform data, we strongly recommend using the FULL recovery model in MSSQL. This model ensures that all transactions are fully recorded in the transaction log file, preserving the log sequence for database restore operations. Unlike the SIMPLE recovery model, the FULL recovery model supports point-in-time restore, page restore, and file restore. The SIMPLE recovery model, while easier to manage, is not loss-less and does not support transaction log backups. This could lead to data loss, which is unacceptable for databases containing TPP data. For more information on the benefits of each model, please refer to Microsoft's documentation on SQL Server Recovery Models.
Database maintenance plan	Minimum weekly rebuild of table indexes - Rebuilding and reorganizing indexes https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes - Perform index operations online (requires Enterprise Edition) https://docs.microsoft.com/en-us/sql/relational-databases/indexes/perform-index-operations-online The performance of index operations online is the major benefit of using MS SQL Enterprise edition rather than Standard edition. With Standard edition, you can only rebuild and reorganize indexes (a recommended weekly manual task) by taking your database server offline, resulting in an outage of Venafi Platform. Enterprise edition allows Venafi Platform to perform these maintenance tasks automatically and in the background with the service remaining active. For help choose the best edition for you, see "Which edition of Microsoft SQL Server should I use?" on page 59

Cloud hosting using Amazon RDS, Azure SQL managed Instance, or Google Cloud SQL

If you want to host Venafi Platform in a cloud data center, you can pick between Amazon RDS, Azure SQL Managed Instance, or Google Cloud SQL. Support for these cloud providers is described in the following table.

IMPORTANT If you use a cloud server for Trust Protection Platform, you should use it for both the database and the Venafi Platform servers. *We do not recommend splitting between a cloud provider and on-prem.*

NOTE Azure SQL Single Database and Azure SQL Elastic pool products are not compatible with Venafi Platform. Additionally Azure SQL Managed Instance *does NOT* support Azure Active Directory authentication for Trust Protection Platform.

In the table below, values are given for specific levels, showing you the minimum system requirements based on the bigger of how many active certificates and SSH keys you have.

- Level 1: Minimum requirements for up to 50k active certificates and 1k SSH servers
- Level 2: Minimum requirements for up to 250k active certificates and 5k SSH servers
- Level 3: Minimum requirements for up to 1M active certificates and 20k SSH servers

For example, if you have 40,000 active certificates and 3,000 SSH servers, you would need to meet the Level 2 requirements since the number of SSH servers exceeds the level 1 allowance.

Feature	Amazon RDS support	Azure SQL Managed Instance support	Google Cloud Database support
Use case	■ Production ■ Development ■ Test	■ Production ■ Development ■ Test	■ Production ■ Development ■ Test
Processor	■ Level 1: 4 processing cores ■ Level 2: 16 processing cores ■ Level 3: 32 processing cores	■ Level 1: 4 processing cores General Purpose ■ Level 2: 16 processing cores General	■ Level 1: 4 processing cores ■ Level 2: 16 processing cores ■ Level 3: 32 processing cores

Feature	Amazon RDS support	Azure SQL Managed Instance support	Google Cloud Database support
		Purpose	cores
		Level 3: 32 processing cores Business Critical	
DB engine version	When selecting the database version, pick the latest version supported by both Venafi Platform and Amazon RDS.	Azure manages the SQL version, and always uses the latest production version of SQL Enterprise Edition.	When selecting the database version, pick the latest version supported by both Venafi and Google Cloud Database.
Microsoft SQL Server edition Info...¹ Help me decide	- Level 1: Enterprise (recommended) and Standard (supported) - Level 2: Enterprise (recommended) and Standard (supported) - Level 3: Enterprise (required)	Based on package choice	- Level 1: Enterprise (recommended) and Standard (supported) - Level 2: Enterprise (recommended) and Standard (supported) - Level 3: Enterprise (required)

¹While both Enterprise and Standard editions are tested and supported by Venafi Support, the Standard edition has some limitations including indexing and performance.

Feature	Amazon RDS support	Azure SQL Managed Instance support	Google Cloud Database support
DB Instance Class	- Level 1: db.m4.xlarge - Level 2: db.m4.4xlarge - Level 3: db.m4.10xlarge	N/A	High Memory
Memory	- Level 1: 16 GB - Level 2: 32 GB - Level 3: 64 GB	Based on package choice	- Level 1: 16 GB - Level 2: 32 GB - Level 3: 64 GB
Database storage	- Level 1: 50 GB - Level 2: 250 GB - Level 3: 1 TB	- Level 1: 50 GB - Level 2: 250 GB - Level 3: 1 TB	- Level 1: 50 GB - Level 2: 250 GB - Level 3: 1 TB
Multi -AZ deployment	AlwaysOn (supported)	Use failover as secondary (built on top of AlwaysOn)	High Availability (supported)
Storage type	Provisioned iOps (SSD)	N/A	SSD
Disk I/O per second - Provisioned iOPS	- Level 1: 5,000 sustained baseline IOPS - Level 2: 10,000 sustained baseline IOPS - Level 3: 20,000 sustained	N/A	Based on machine type

NOTE All values assume a 90-day log retention period. If your retention period is longer, you will need more storage.

Feature	Amazon RDS support	Azure SQL Managed Instance support	Google Cloud Database support
baseline IOPS			
Public accessibility	No	No	Yes (if configured)
Microsoft SQL Server Windows Authentication	Untested	Not supported	Untested
Deletion protection	Enabled	Enabled	N/A
Additional Notes	Using AWS RDS Multi-AZ (availability zone) with Venafi Platform requires special considerations, including a virtual private cloud with both public and private subnets. Contact Venafi Customer Support for more details.		
		Azure Active Directory authentication is NOT supported.	

Locally Hosted MSSQL Requirements

In the table below, values are given for specific levels, showing you the minimum system requirements based on the bigger of how many active certificates and SSH keys you have.

- Level 1: Minimum requirements for up to 50k active certificates and 1k SSH servers
- Level 2: Minimum requirements for up to 250k active certificates and 5k SSH servers
- Level 3: Minimum requirements for up to 1M active certificates and 20k SSH servers

EXAMPLE If you have 40,000 active certificates and 3,000 SSH servers, you would need to meet Level 2 requirements since the number of SSH servers exceeds the level 1 allowance.

Feature	Level 1	Level 2	Level 3
Processor	4 processing cores	16 processing cores	32 processing cores
Memory	16 GB	32 GB	64 GB
Disk I/O per second (IOPS)	5,000 sustained baseline IOPS	10,000 sustained baseline IOPS	20,000 sustained baseline IOPS
Database Storage	50 GB	250 GB	1 TB
NOTE All values assume a 90-day log retention period. If your retention period is longer, you will need more storage.			
Microsoft SQL Server editions	- Enterprise (Recommended) - Standard (Compatible)	- Enterprise (Recommended) - Standard (Compatible)	Enterprise (Required)

[More info...](#)¹ | [Help me decide](#)

Supported HSMs

Venafi Trust Protection Platform supports integrations with Hardware Security Modules (HSMs) to encrypt private keys, credentials, and other secrets stored in the database. You can also use the HSM integration for the central generation of private keys when you also have Venafi Advanced Key Protect. If either of these use cases apply to you, use the following tables to see what HSMs are *supported* and which HSMs have been self-certified from their vendors as being *compatible*.

IMPORTANT Venafi recommends you consult the partner documentation for minimum supported versions.

¹While both Enterprise and Standard editions are tested and supported by Venafi Support, the Standard edition has some limitations including indexing and performance.

TIP The following tables show vendor support for generating private keys. In all cases, this refers to Hardware Central Key Generation. Learn more about [Supported methods of key generation](#).

Supported HSM	Docs	Encrypt Secrets	HCKG for private keys ¹	Code Signing Certificate Private Key Storage ²
Entrust nShield Connect HSM	Partner PDF			
Thales SafeNet Luna SA (including Azure Dedicated HSM)	Partner Docs			

Vendor Self-Certified HSMs

NOTE The HSM Partners on the list below have gone through the process of self-certification. This process involves testing the specific PKCS#11 mechanisms that Trust Protection Platform uses when an HSM is used to protect things like private keys and credential objects, and when Advanced Key Protect is enabled.

Self-certification means that the partner has done the testing and proven successful results and integration with Venafi. Successful self-certification results indicate that the integration will work as expected. The HSM vendor may need to be engaged if something is working unexpectedly. Consult the partner's documentation to know what firmware version requirement is.

¹Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.

²Requires **Venafi Advanced Key Protect** add-on module

HSM Vendor <i>HSM Product</i>	Docs	Encrypt Secrets	HCKG for private keys ¹	Code Signing Certificate Private Key Storage ²
Atos <i>Trustway Protezione</i>	PDF (no public link; contact vendor)			
AWS CloudHSM	Venafi Docs			
Crypto4A <i>QxEDGE</i>				
Entrust <i>Entrust nShield as a Service</i>	Partner Docs			
Fortanix <i>Fortanix DSM</i>	Partner Docs			
FutureX <i>Vectra Plus</i>	Partner Docs			
Gradient <i>KeyConnect</i>				
Securosys <i>Primus HSM and Cloud HSM Service</i>	Partner Docs (Login required)			

¹Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.

²Requires **Venafi Advanced Key Protect** add-on module

HSM Vendor <i>HSM Product</i>	Docs	Encrypt Secrets	HCKG for private keys ¹	Code Signing Certificate Private Key Storage ²
Thales TCT <i>T-Series Luna</i>	Partner Docs			
Thales <i>Data Protection on Demand</i>	Partner Docs			
Utimaco <i>CryptoServer</i>	Partner Docs (Login required)			

For information on using HSMs to encrypt secrets, see [Using HSM-protected encryption keys](#).

For information on using HSMs for central private key generation, see [Hardware Central key generation with Venafi Advanced Key Protect](#).

For information on using HSMs for remote key generation, see [Hardware remote key generation with Venafi Advanced Key Protect](#).

Port and network access

Port requirements

Depending on your environment, Trust Protection Platform can use the following ports:

¹Support in this column indicates the vendor can generate private keys using Hardware Central Key Generation (HCKG). Requires **Venafi Advanced Key Protect** add-on module.

²Requires **Venafi Advanced Key Protect** add-on module

Port	Description
Default Port Assignments	
80	While Venafi Platform provides several methods of ensuring encryption of traffic, Port 80 binding is ONLY required if you are using SCEP or the Time Stamp Service endpoints, as these features require http access to the internet to function correctly. If you are not using SCEP, and you don't care if the Time Stamp Service endpoints in CodeSign Protect can get time stamping data, you can disable Port 80 binding in IIS. All other Venafi web services will continue to function if access to port 80 is blocked.
443	Hyper Text Transfer Protocol Secure (HTTPS) should be enabled if Policy Tree is secured with a certificate.
50443	This port is used by Trust Protection Platform to handle certificate requests via Enrollment Over Secure Transport (EST) protocol. Allow this port only on servers which will handle such requests.
8883	This is the IANA-assigned port for encrypted (TLS) MQTT connections between servers in the cluster using the Message Bus feature. By default, Message Bus uses this encrypted port. If you opt for unencrypted communication, the IANA-assigned port is 1883.
Operational Port Assignments	
135	Trust Protection Platform communicates with the Microsoft Certificate Services and the server hosting Internet Information Services over DCOM. The default DCOM port is 135 (dynamic port range 49152-65535). Trust Protection Platform contacts the IIS application on port 135; however, the application returns its response on a different port. This can pose a problem in a firewall environment. For information on configuring DCOM with firewalls, see the following Microsoft Technical Document: http://support.microsoft.com/kb/154596.
21	Port 21 can be used for sending reports via the FTP protocol. Reports can also be sent using the SMB protocol (port 445).
22	Trust Protection Platform uses the Secure Shell protocol (SSH) to communicate with servers and appliances. The default SSH port is 22. SCP and SFTP run as subsystems of SSH on port 22. Trust Protection Platform supports Open SSH and Tectia SSH versions 4 and 5.3.x.
25, 587	Trust Protection Platform uses the Simple Message Transfer Protocol (SMTP) to communicate with a configured email server to send email notifications. The default SMTP port is 25.

Port	Description
161	Trust Protection Platform uses the Simple Network Management Protocol (SNMP) channel to send selected events to an SNMP management system via an SNMP trap.
445	Port 445 can be used for sending reports via the SMB protocol. Reports can also be sent using the FTP protocol (port 21).
514	The Venafi Log server can send log messages to a syslog server. By default, the Syslog channel uses UDP port 514, but an administrator may configure an alternate port in the Syslog channel configuration. The Log server can also use TLS for sending Syslog messages, if configured.

For more information, see [About syslog channels](#).

Default Database Ports	
1433	For more information on running the Trust Protection Platform database on a Microsoft SQL system, see " Setting up your Microsoft SQL database server " on page 60.

Network access requirements

Platform requirements

There are a number of systems that require network access to be enabled for Trust Protection Platform to run.

- All Venafi servers need access to the database server
- If using an HSM to (1) encrypt private keys, credentials, and other secrets stored in the Venafi database, or (2) for the central generation or storage of private keys, all Venafi servers need access to the HSM.
- If using an identity provider, like Active Directory or LDAP, all Venafi servers need network access to the identity infrastructure.
- Each Venafi server that has the Event Processing component enabled must have access to the configured logging channels. For example, email server, syslog, SMTP, etc.
- For each Venafi server that has a web service enabled (e.g. UI consoles, Web SDK, Agent service, etc.), all clients that are connecting to the service must have network access to the Venafi server, either directly or through a proxy.

Feature-specific requirements

Most features in Trust Protection Platform can be configured to only use a subset of servers to use that feature. For example, when integrating with a certificate authority, the Venafi server(s) integrated with that certificate authority need network access to connect to that certificate authority, but other servers in your cluster would not need that access.

There are three ways you can control what Venafi servers need access:

- Processing engines. For more information see [Management Zones](#).
- Network discovery zones. For more information see [Configuring discovery zones](#).
- Turning off the associated component on a specific server's Venafi Configuration Console. For more information see "[Trust Protection Platform components](#)" on page 80.

Most product features have a Network Access component for the feature. We recommend you review what features you plan to use, as well as which Venafi server(s) will be responsible for these features, and configure network access accordingly.

Venafi MMC Snap-in Collection

The Venafi Configuration Console is built upon the Microsoft Management Console (MMC) Framework. Some of the nodes, such as the Venafi Event Viewer and the Code Signing are snap-ins that are available to be installed on other Windows servers and workstations, even if they are not setup to be Venafi servers. If you plan leverage this functionality, it can only be installed on Windows systems that meet the following requirements:

- .NET 4.7.2
- Windows 8.1 or later or Windows Server 2016 or later

Code Signing Workstation Clients

Venafi CodeSign Protect requires the use of code signing clients that are installed on development workstations and/or build pipeline servers. These workstations or servers have the following requirements:

- Windows
 - .NET Framework 4.8
 - Windows 10 or later
 - Windows Server 2016 or later
- Linux versions tested by Venafi
 - Debian 9 and later
 - Ubuntu 16.04 and later
 - CentOS Stream 8 and later
 - Red Hat Enterprise Linux (RHEL) 7 and later
- macOS
 - Monterey 12 and later

Server Agent

Venafi Server Agent

Venafi Server Agents are an optional component of the Venafi Trust Protection Platform. They facilitate the discovery, rotation, and validation of Certificates or SSH keys for the **TLS Protect** and **SSH Protect** products respectively. Both products support the agent and agentless technology for discovery, rotation, and validation. Review [About certificate installation methods: agentless versus agent](#) and decide if you are going to be using agent, agentless, or both technologies in your deployment.

Unless otherwise specified, all updates, patches, editions, and service packs (SPs) for a listed operating system version are supported. The 64-bit architecture is supported across most platforms (see below). IPv6 is supported on all operating systems.

NOTE Venafi typically releases major software updates twice a year. Operating system vendors release new SPs and patches regularly. Releases rarely occur at the same time.

Supported Operating Systems

- Microsoft Windows 10, Microsoft Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 (64-bit only), and Windows Server 2022.

Before installing the Server Agent, verify that target systems use one of the supported x86-64 operating systems as noted above.

- All supported versions of Windows Server require the Visual C++ Redistributable package. You can download the latest version of the redistributable package from the official Microsoft website at learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist.
- The Server Agent requires .NET 4.8 or later on all Windows versions.
- AIX 7.1 (PPC) and AIX 7.2 (PPC)
- Solaris 10 (SPARC), and Solaris 11 (SPARC)
- Red Hat Enterprise Linux (RHEL) 6, RHEL 7, RHEL 8, and RHEL 9 (64-bit only)
- Community Enterprise Operating System (CentOS) 6, CentOS 7, and CentOS 8 (64-bit only)
- SUSE Linux Enterprise Server versions 11 and 12 (64-bit only)

Compatible Keystores

For information about compatible keystores for certificate installation, see [Server Agent-supported keystores](#) in the *Server Agent Installation and Configuration Guide*.

Disk Space Requirements

200 MB free disk space (150 MB for agent and 50 MB to store results waiting to be returned to the Trust Protection Platform server).

IMPORTANT If you are upgrading the Server Agent or Trust Protection Platform, see [Before upgrading](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Venafi Certificate Authority Drivers

Certificate Authority integrations are a required component of the TLS Protect and CodeSign Protect products for any level of automation beyond discovery and expiration monitoring. Verify that your current Certificate Authorities are on the list of supported integrations below. If not, they may be supported by a third party through our Adaptable Framework.

Supported Enterprise Certificate Authorities

The following internal CA drivers are supported on the past four versions of Trust Protection Platform:

- Adaptable CA
 - Includes a reference sample of DigiCert PKI Platform (Magnum).
- Microsoft Standalone CA
- Microsoft Enterprise CA (ADCS)
- OpenSSL
- OpenTrust Enterprise PKI
- RedHat Certificate System
- RSA Certificate Manager
- DigiCert PKI Platform
- Verizon CyberTrust UniCERT

TIP For a complete list of supported version numbers, see [Supported integrations with Trust Protection Platform](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Supported Public Trust Certificate Authorities

The following external CA drivers are supported on the past four versions of Trust Protection Platform and all include an API interface and are cloud-based hosting platforms:

- Amazon Certificate Manager (ACM)
- Sectigo Certificate Manager (SCM)

- DigiCert CertCentral
- Entrust Certificate Services
- GeoTrust Reseller
- GeoTrust TrueFlex (GESC)
- GlobalSign MSSL
- HID PKIaaS
- QuoVadis
- Symantec Managed PKI for SSL
- Thawte
- VikingCloud

TIP For a complete list of supported version numbers, see [Supported integrations with Trust Protection Platform](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Supported CodeSign Protect Certificate Authorities

- DigiCert
- Entrust Certificate Service
- Microsoft CA
- Microsoft CA Pool

Provisioning (Certificate Installation) Drivers

Agentless Provisioning drivers support the automatic installation of TLS certificates to their host systems and are a feature of TLS Protect that require a Trust Force™ license for each endpoint you install to. Below is a list of natively supported integrations with certificate keystores, applications, cloud services, and enterprise appliances. If your application is not listed, it does not necessarily mean that automatic installation cannot be achieved. For example, provisioning to a Tomcat web server is possible using the Java Keystore driver. Other integrations are possible using the Adaptable Framework through third parties and the Venafi Marketplace. Review the list of what drivers you plan to use as part of your deployment.

Supported Keystores and Applications for Provisioning (Certificate Installation)

The following provisioning drivers are supported on the past five versions of Trust Protection Platform, except where noted:

- Adaptable Application
- Apache/PEM (OpenSSL)
- IBM Global Security Kit (GSK)
- Java Keystore (JKS and JCEKS)
- Microsoft CAPI
- Microsoft IIS
- Network Security Services (Oracle iPlanet)
- PKCS#12

See [About CSR-supported formats](#) in the Certificate Authority and Hosting Platform Integration Guide for more information.

TIP For a complete list of supported version numbers, see [Supported integrations with Trust Protection Platform](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

NOTE For a list of supported keystores to which you can provision using the Server Agent, see [Server Agent supported keystores](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Supported Appliances

The following appliance drivers are supported on Trust Protection Platform:

- Amazon Web Services IAM/ELB/CloudFront
- Apache
- Azure Key Vault (Microsoft)
- Blue Coat SSL Visibility Appliance
- CAPI (IIS 7+)
- Citrix NetScaler MPX (with HSM)

- Citrix NetScaler VPX
- F5 Big-IP F5 LTM Advanced
- Google Cloud Load Balancer (external proxies only)
- HashiCorp Vault PKI
- IBM GSK
- IBM Sterling Connect:Direct
- IBM WebSphere DataPower
- Imperva MX (doesn't support file validation)
- iPlanet
- JKS
- Juniper SA/MAG Series
- Palo Alto Networks Next Generation Firewall
- PEM
- Riverbed SteelHead WAN Optimizer
- Tealeaf PCA (Passive Capture Appliance)
- VAM nShield

TIP For a complete list of supported version numbers, see [Supported integrations with Trust Protection Platform](#) in the *Certificate Authority and Hosting Platform Integration Guide*.

Supported browsers and supported vendors, products, and versions

Supported and Compatible Web Browsers

Status	Browser
Supported	Microsoft Edge (Chromium, latest version) and Google Chrome (latest version)
Compatible	Firefox 78 ESR

Monitor Resolution

Minimum supported monitor resolution requirement: 1280 x 1024.

Supported Vendors, Products, and Versions

Vendor	Supported Products	Supported Versions*	Integration Types
Amazon	Amazon Certificate Manager (ACM)		Certificate Authority
Amazon	Amazon Web Services (AWS)	ACM, IAM, ALB, ELB, CloudFront	Cloud Service
Apache	HTTP Server	2.2 and 2.4	Application
Bouncy Castle	Clients using BC bcpkix library	1.64	Certificate Enrollment via EST Protocol
Cisco	libest (Client)	1.1.0	Certificate Enrollment via EST Protocol
Cisco	IOS	15.7(3)M3	Certificate Enrollment via EST Protocol
Citrix	NetScaler VPX	14.1, 13.1 build 42.47, 13.0 build 58.32	Network Appliance
Citrix	NetScaler MPX w/HSM	v13.0 build 58.32	Network Appliance
Compuware	VAM w/nShield 6000e F2	V11.05.1245 (64 bit)	Network Appliance
CyberArk	Enterprise Password Vault	10.5, 11, 12	Credential Provider
Dell	iDRAC 8 (using RACADM 8.3)**	2.41.40.40 firmware	IoT
DigiCert	DigiCert CertCentral	NA	Certificate Authority

Vendor	Supported Products	Supported Versions*	Integration Types
Entrust	Entrust Certificate Services	NA	Certificate Authority
Entrust nShield	Entrust nShield Connect HSM	12.40.2 (client; minimum version)	Hardware Security Module
F5	Big-IP Local Traffic Manager (LTM) / Application Delivery Controller (ADC)	15.1.9.1 build 0.0.5, 16.1.3.5 build 0.0.5, 17.1.0.2 build 0.0.2	Network Appliance
GeoTrust	GeoTrust Reseller	NA	Certificate Authority
GlobalSign	GlobalSign MSSL	NA	Certificate Authority
Hewlett-Packard (HP)	iLO 4 (using HPQLOCFG 1.5)**	2.50 firmware	IoT
HID PKIaaS	HID PKIaaS	NA	Certificate Authority
IBM	WebSphere DataPower IDG	10.0.1, 10.5.0	Network Appliance
IBM	TeaLeaf Passive Capture Application (PCA)	v2 3400	Appliance
IBM	Sterling Connect:Direct with Secure+	6.0x, 6.1x, 6.2x for Windows and 6.0x, 6.1x, 6.2x for UNIX	Application
IBM	Global Security Kit (GSK)	7.0.3.15, 7.0.4.20 (gsk7cmd, gsk7capicmd & iKeyMan); 8.0.14.34 (gsk8capicmd)	Keystore
Imperva	MX	13.6	Appliance

Vendor	Supported Products	Supported Versions*	Integration Types
Microsoft	Active Directory Certificate Services (ADCS)	Enterprise or Standalone CA running on Windows Server 2003-2012, 2016, 2019, and 2022	Certificate Authority
Microsoft	Internet Information Services (IIS)	8.0, 8.5, 10.0.1607, and 10.0.1809	Application
Microsoft	Azure	Key Vault, Web App	Cloud Service
Microsoft	Windows Certificate Store (CAPI)	Windows Server 2012, KeyStore 2012 R2, 2016, and 2019	
Mozilla	Network Security Services (NSS) For more information, visit https://en.wikipedia.org/wiki/Network_Security_Services .	3.x	Keystore
OpenSSL	PEM	NA	Keystore
OpenSSL	OpenSSL CA	1.0.0, 3.0.0	Certificate Authority
OpenTrust	Enterprise PKI	4.7.1	Certificate Authority
Oracle	Java Keystore (JKS and JCEKS)	1.6, 1.7, 1.8	Keystore
Oracle	Sun Java System Web Server / Oracle iPlanet Web Server For more information, visit https://en.wikipedia.org/wiki/Oracle_iPlanet_Web_Server .	6.1, 7.0	Application
Palo Alto Networks	Next Gen Firewall	10.2.7+ and 11.1.x+	Appliance
QuoVadis	QuoVadis	NA	Certificate Authority

Vendor	Supported Products	Supported Versions*	Integration Types
RedHat	Red Hat Certificate System	8.1	Certificate Authority
Riverbed	SteelHead WAN Optimizer	VCX555H 9.0.0b	Appliance
RSA Security	RSA Certificate Manager	6.8 and 6.9	Certificate Authority
RSA Security	PKCS#12	NA	Keystore
Sectigo	Sectigo Certificate Manager (CCM)	NA	Certificate Authority
Symantec	Symantec Managed PKI for SSL	NA	Certificate Authority
Symantec	DigiCert PKI Platform***	NA	Certificate Authority
Symantec (Blue Coat)	SSL Visibility Appliance	3.11.3.1 (Remote API 2.9)	Network Appliance
Thales	estclient	1.0.1	Certificate Enrollment via EST Protocol
Thales	SafeNet Luna SA	6.22 (client)	Hardware Security Module
Verizon	CyberTrust UniCERT	5.3.4	Certificate Authority
VikingCloud	VikingCloud	NA	Certificate Authority

* Venafi Labs has tested these versions. Other versions might be compatible but are not supported by Venafi.

** For Dell iDRAC and HP iLO, refer to the Adaptable Application driver reference samples. See [Adaptable Application](#).

*** DigiCert PKI Platform is provided as a supported reference sample for the Adaptable CA driver. See [Adaptable CA](#).

2

Installing Trust Protection Platform

Review this overview before you start the Venafi Trust Protection Platform™ installation.

BEST PRACTICE Before you install Trust Protection Platform 25.1, please review [Important Considerations before upgrading Venafi Platform](#).

To install Venafi Trust Protection Platform

1. Prepare your network for Trust Protection Platform.
For specific instructions, see ["Preparing your environment for the Venafi Platform"](#) on page 41.
2. Configure your database and database accounts.
For more information, see ["Preparing the database server"](#) on page 59.
3. Install Trust Protection Platform.
For specific instructions, see ["Installing and Configuring Venafi servers"](#) on page 66.
4. Install Trust Protection Platform on additional servers, as needed.
5. (Recommended) Replace the default self-signed certificate (Venafi Operational Certificate) with a fully trusted end-entity certificate.

To learn more about the Venafi Operational Certificate, see ["Securing Trust Protection Platform's web servers" on page 114](#).

To learn how to replace the Venafi Operational Certificate, see [Replacing the Venafi Operational Certificate \(VOC\) with your own CA-signed certificate](#).

6. After the installation is complete, see [Network and local certificate management configuration overview](#) in the *Venafi Trust Protection Platform Certificate Management Guide* for an outline of the steps required to configure Trust Protection Platform to manage network and local certificates in your encryption environment.

Carefully review ["Installing and Configuring Venafi servers" on page 66](#) before launching the installation process.

This chapter contains the following topics:

Preparing your environment for the Venafi Platform	41
Preparing the database server	59
Installing and Configuring Venafi servers	66
Command line installation and configuration	87
Post-installation procedures	113

Preparing your environment for the Venafi Platform

This section shows you how to prepare the Windows servers and meet the requirements for a successful installation of Venafi Trust Protection Platform. This is a great place to start before you begin installing software.

TIP You can save valuable time in assessing and installing system prerequisites by running the Prereq Check Script and the Base Configuration Utility available at <https://download.venafi.com/>. After signing in, expand **PS Utilities** and download the following:

- Prereq Check Script¹
- Base Configuration Utility²

The steps for successfully preparing for an installation of Venafi Trust Protection Platform are listed below. More details about each step can be found in this chapter.

1. Carefully review the system requirements and make a note of the requirements that are applicable to your planned deployment and environment. See "Reviewing system requirements before installation" on the next page.
2. Determine the number of Venafi servers you will deploy and the purpose of each server. See "Determining the number of Windows servers needed" on the next page
3. "Deploy and configure the Windows servers" on the next page.
4. Ensure "Network connectivity requirements" on page 48 are met including routing, firewall, and port access that are applicable to your planned deployment and environment.

To assist you in tracking these steps for deploying and configuring your Windows servers, we've provided an "Installation preparation worksheet" on page 53.

¹A PowerShell script that rapidly verifies whether or not all Venafi Platform prerequisites are installed already and reports which ones are not. You can even use the optional `Install` parameter to automatically install some missing items and remove the IIS default web site, something typically done manually following installation of the Venafi Platform.

²Download and run this utility to set most of the common post-install checklist requirements automatically, including the creation of best-practice policy tree folders, workflows, notifications, and discovery placement rules.

Reviewing system requirements before installation

Carefully review the list of system requirements for installing and configuring Venafi Trust Protection Platform. Some requirements are for all deployments. Other requirements give options based on scale, such as database server resources and number of Venafi servers. Some requirements are optional based on Venafi products and feature you plan to use in the deployment you are designing.

As you review the requirements carefully, note which requirements will apply to your deployment so you can easily reference them throughout the deployment process. You might find the ["Installation preparation worksheet" on page 53](#) useful as you review the requirements.

For a detailed list of requirements, see ["System requirements for Venafi components" on page 7](#).

Determining the number of Windows servers needed

In the System Requirements, the section ["Number of Trust Protection Platform servers needed" on page 8](#) gives information about the base number of Venafi servers your deployment requires. This value is based on the total number of certificates and SSH keysets you plan to actively monitor and manage. If Server Agents are used, then additional Venafi servers are needed.

If your network is complex, you will likely need more Venafi servers. For example, for network or onboard discovery of certificates and SSH keys, at least one Venafi server will require network access to the systems you wish to scan. If you plan to do validation, rotation, and installation of certificates and keys, those servers also need network access over the management port of the target system. If you want to provide high availability or disaster recovery service for the platform, you will need additional servers for those features.

If you'd like help figuring out your best deployment size, feel free to reach out to your assigned Venafi Account Executive who will put you in touch with Venafi Professional Services. In general, small deployments will frequently have between two and four Venafi servers. Larger deployments sometimes have 10 or more Venafi servers.

Deploy and configure the Windows servers

Here are the high level steps to deploy and configure each Windows server that will become a Venafi server.

1. Review the hardware and operating system requirements for the Windows servers.

Hardware and operating system requirements for Windows servers

Feature	Requirement
Processor	4 processing cores
Memory	16 GB RAM
Disk Space (for the Trust Protection Platform application)	5 GB
	The Trust Protection Platform application can be installed on a secondary partition.

Feature	Requirement
Operating Systems	- Microsoft Windows Server 2022 (server with user interface) is <i>supported</i> (and required if you want to use TLS 1.3). - Microsoft Windows Server 2019 (server with user interface) is <i>supported</i>. - Microsoft Windows Server 2016 (server with user interface) is <i>supported</i>.
	Trust Protection Platform only supports English Language Installation Media from Microsoft. While it does support region setting configurations to ensure that date and times appear correctly, the Windows servers on which you install Trust Protection Platform must be derived from Windows English installation media.

- Where applicable, join your Windows server to your Active Directory domain.

Join Windows servers to Active Directory

While a connection to Active Directory is not required for base functionality, it is required to use certain features such as Windows integrated authentication.

Windows integrated authentication is supported in two ways in Trust Protection Platform:

- Authentication to the database from the Venafi servers.
- User authentication to the web interface for single sign-on (SSO).

- Enable web services, if needed.

Enable web services on required servers

For each Windows server, decide if it is going to be supporting inbound web services or not. If the server will support web services, then the required windows server role and corresponding components are followed as outlined in the System Requirements guide.

IIS can start its default web site before the Venafi site on the server, preventing the Venafi site from starting. You should remove the default web site.

Some examples of web services are the Web Console, Web SDK, supporting connectivity from our agents, as well as some certificate protocols like ACME or SCEP. However, if you are deploying a Venafi server to a segmented network to discovery, validate, and install certificates and ssh keys, plan on leveraging partitioning to ensure that a particular Venafi server communicates with the internet or various network segments, then it is possible to configure those Venafi servers with no web services. In those cases, the IIS role does not need to be installed.

Feature	Requirement
Web Server Roles (Venafi web services enabled)	Install the following required Microsoft Internet Information (IIS) web server roles: ◦ 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
Windows Server Roles	Microsoft Windows 2022 Server
(Web Server\Application Development\ .NET Extensibility)	◦ ASP.NET 4.8 ◦ ISAPI Extensions ◦ ISAPI Filters

Feature	Requirement
	◦ .NET Extensibility 4.8
	Microsoft Windows 2019 Server
	◦ ASP.NET 4.6 ◦ ISAPI Extensions ◦ ISAPI Filters ◦ .NET Extensibility 4.6
	Microsoft Windows 2016
	◦ ASP.NET 4.5 ◦ ISAPI Extensions ◦ ISAPI Filters ◦ .NET Extensibility 4.5
Microsoft runtime libraries	You need to install both the following Visual C++ Runtime libraries: ◦ 32-bit version ◦ 64-bit version For more information, see the following from Microsoft: Latest supported Visual C++ Redistributable downloads
Windows service dependencies	The following services should not be disabled: ◦ CNG Key Isolation (for elliptic curve key operations)

Feature	Requirement
IIS 7.5 Add-On	Microsoft URL Rewrite Module 2.1
.NET Framework (Venafi web services enabled)	.NET Framework 4.8 is <i>required</i> for all OS versions. Download .NET Framework 4.8 from https://dotnet.microsoft.com/download/dotnet-framework/net48.
Port 80 Binding Requirements	If you are using SCEP (Simple Certificate Enrollment Protocol), you must allow port 80 binding. SCEP will not work without port 80 binding. Additionally, the timestamping service requires port 80. If access to port 80 is blocked, the Time Stamp Service endpoints in CodeSign Protect will not be able to get timestamping data. If you are not using SCEP, and you don't care about access to the Time Stamp Service Endpoints, you can disable access on Port 80.

4. Apply correct permissions for domain service accounts if leveraging Windows integrated authentication.

Apply correct permissions for domain service accounts

For Windows Servers joined to the domain, you are likely to leverage Windows Integrated Authentication to authenticate to the Venafi database on your Microsoft SQL Server. You will need two domain services accounts and they need to be given the correct permissions on each Windows Server.

If you haven't done so yet, create the accounts. Then apply the correct permissions in AD. For specific permissions details, see "[Windows permissions for database service accounts](#)" on page 64.

5. If your industry requires, enable FIPS on your Windows server.

Enable FIPS (only recommended if required by your industry)

Venafi Trust Protection Platform support Windows servers with Federal Information Processing Standard (FIPS) enabled.

FIPS Resources

- [Why We're Not Recommending "FIPS Mode" Anymore \(from Microsoft Security Baselines Blog\)](#)¹
- [Microsoft's approach to FIPS validation \(from Microsoft Windows documentation\)](#)²

IMPORTANT Because FIPS is not supported for ACMEv2, you cannot have FIPS enabled on any server that is used for ACMEv2.

How to Enable FIPS on Windows Servers

- On each server, open the **Local Group Policy Editor** by opening the `gpedit.msc` snap-in.
 - In the snap-in navigate to **Local Group Policy Editor > Computer Configuration > Windows Setting > Security Settings > Local Policies > Security Options**.
 - Find the policy **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
 - Change the option from **Disabled** to **Enabled**.
6. Verify prerequisite software and components are installed.

Verify prerequisite software and components are installed

Venafi Professional Services maintains a script you can run on your Venafi servers to verify the appropriate prerequisites have been met for the server, and optionally install and configure any missing components. The accompanying README.txt file provides detailed information about using the script. The [script and documentation](#)³ are available on Venafi's Downloads site.

If you choose not to run the script, we strongly recommend you look at the Third Party folder contained the Venafi Trust Protection Platform zip for helpful links for finding required common components that must be installed. The **URL Rewrite Module** only needs to be installed on Venafi servers configured for inbound web services. (See step 3, above.)

Install HSM client on Venafi server

¹<https://techcommunity.microsoft.com/t5/microsoft-security-baselines/why-we-8217-re-not-recommending-8220-fips-mode-8221-anymore/ba-p/701037>

²<https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation#using-windows-in-a-fips-140-2-approved-mode-of-operation>

³[https://download.venafi.com/PS Utilities/PreReq Script/](https://download.venafi.com/PS%20Utilities/PreReq%20Script/)

Trust Protection Platform is a native 64-bit application. When integrating with HSMs to (1) encrypt private keys, credentials, and other secrets stored in the Venafi database, or (2) for the central generation or storage of private keys, you must install the 64-bit version of the HSM vendor's client software on each Venafi server in your deployment. These settings must be configured identically on all Venafi servers in the deployment. During installation of the Trust Protection Platform software, you will need to provide details on the HSM vendor client library.

For example:

Trust Protection Platform requires access to the 64-bit version of Cryptoki DLL.

For SafeNet Luna SA devices, this is the path to the `cryptoki.dll` file.

For Entrust nShield Connect HSM devices, this is the path to the `cknfast.dll` file.

After selecting the DLL, click **Load Slots**. Trust Protection Platform will query the HSM and return the available slots.

IMPORTANT Trust Protection Platform requires the path to the DLL file to initialize the connection to the HSM device. This path will be used for all Trust Protection Platform servers in the cluster (connected to the same database). All servers in the cluster must have their DLL file in the same location.

Network connectivity requirements

IPv6 Support

Trust Protection Platform supports the IPv6 protocol across the product with one exception: for network discovery, IPv6 is not supported for network discovery jobs.

Network access requirements

Platform requirements

There are a number of systems that require network access to be enabled for Trust Protection Platform to run.

- All Venafi servers need access to the database server
- If using an HSM to (1) encrypt private keys, credentials, and other secrets stored in the Venafi database, or (2) for the central generation or storage of private keys, all Venafi servers need access to the HSM.

- If using an identity provider, like Active Directory or LDAP, all Venafi servers need network access to the identity infrastructure.
- Each Venafi server that has the Event Processing component enabled must have access to the configured logging channels. For example, email server, syslog, SMTP, etc.
- For each Venafi server that has a web service enabled (e.g. UI consoles, Web SDK, Agent service, etc.), all clients that are connecting to the service must have network access to the Venafi server, either directly or through a proxy.

Feature-specific requirements

Most features in Trust Protection Platform can be configured to only use a subset of servers to use that feature. For example, when integrating with a certificate authority, the Venafi server(s) integrated with that certificate authority need network access to connect to that certificate authority, but other servers in your cluster would not need that access.

There are three ways you can control what Venafi servers need access:

- Processing engines. For more information see [Management Zones](#).
- Network discovery zones. For more information see [Configuring discovery zones](#).
- Turning off the associated component on a specific server's Venafi Configuration Console. For more information see ["Trust Protection Platform components" on page 80](#).

Most product features have a Network Access component for the feature. We recommend you review what features you plan to use, as well as which Venafi server(s) will be responsible for these features, and configure network access accordingly.

Port requirements

Depending on your environment, Trust Protection Platform can use the following ports:

Port	Description
------	-------------

Default Port Assignments	
---------------------------------	--

80	While Venafi Platform provides several methods of ensuring encryption of traffic, Port 80 binding is ONLY required if you are using SCEP or the Time Stamp Service endpoints, as these features require http access to the internet to function correctly.
----	--

If you are not using SCEP, and you don't care if the Time Stamp Service endpoints in CodeSign Protect can get time stamping data, you can disable Port 80 binding in IIS.

Port	Description
------	-------------

	All other Venafi web services will continue to function if access to port 80 is blocked.
--	--

443	Hyper Text Transfer Protocol Secure (HTTPS) should be enabled if Policy Tree is secured with a certificate.
-----	---

50443	This port is used by Trust Protection Platform to handle certificate requests via Enrollment Over Secure Transport (EST) protocol. Allow this port only on servers which will handle such requests.
-------	---

8883	This is the IANA-assigned port for encrypted (TLS) MQTT connections between servers in the cluster using the Message Bus feature. By default, Message Bus uses this encrypted port. If you opt for unencrypted communication, the IANA-assigned port is 1883.
------	---

Operational Port Assignments

135	Trust Protection Platform communicates with the Microsoft Certificate Services and the server hosting Internet Information Services over DCOM.
-----	--

The default DCOM port is 135 (dynamic port range 49152-65535). Trust Protection Platform contacts the IIS application on port 135; however, the application returns its response on a different port. This can pose a problem in a firewall environment. For information on configuring DCOM with firewalls, see the following Microsoft Technical Document: <http://support.microsoft.com/kb/154596>.

21	Port 21 can be used for sending reports via the FTP protocol. Reports can also be sent using the SMB protocol (port 445).
----	---

22	Trust Protection Platform uses the Secure Shell protocol (SSH) to communicate with servers and appliances. The default SSH port is 22.
----	--

SCP and SFTP run as subsystems of SSH on port 22.

Trust Protection Platform supports Open SSH and Tectia SSH versions 4 and 5.3.x.

25, 587	Trust Protection Platform uses the Simple Message Transfer Protocol (SMTP) to communicate with a configured email server to send email notifications. The default SMTP port is 25.
---------	--

161	Trust Protection Platform uses the Simple Network Management Protocol (SNMP) channel to send selected events to an SNMP management system via an SNMP trap.
-----	---

445	Port 445 can be used for sending reports via the SMB protocol. Reports can also be sent using the FTP protocol (port 21).
-----	---

514	The Venafi Log server can send log messages to a syslog server. By default, the Syslog channel uses UDP port 514, but an administrator may configure an alternate port in the Syslog channel configuration. The Log server can also use TLS for sending Syslog messages, if configured.
-----	---

Port	Description
	For more information, see About syslog channels .
Default Database Ports	
1433	For more information on running the Trust Protection Platform database on a Microsoft SQL system, see "Setting up your Microsoft SQL database server" on page 60.

Database Encryption

Venafi Platform uses encryption at rest to protect the information stored in your database. There are two options for database encryption: software encryption, and hardware encryption. You must use some combination of the two (hardware, or software, or both).

Understanding your encryption options is important so you know how Venafi Platform is protecting your data.

For more information on encryption drivers and how to configure them, see [Overview of encryption drivers](#).

Software Encryption

If you select software encryption, your database assets will be encrypted using an AES-256 encryption key stored in the Windows registry. You either provide a key, or have Venafi Platform generate a key for you. You must use the same encryption key on all Venafi servers.

To export your software key for backup or to use on another server, you can use the Venafi Configuration Console (VCC), or you can use the command line.

For information on using VCC, see ["Backing up the software encryption key"](#) on page 114.

To backup using the command line, run the following command:

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

Hardware Encryption

If you select hardware encryption, your encryption material will be stored on a hardware security module (HSM), such as one provided by SafeNet Luna SA, Entrust nShield, or other HSM provider.

NOTE While most other uses of HSMs require Venafi Advanced Key Protect (AKP), you can encrypt secrets in your database using an HSM without a license for AKP.

More information on hardware encryption can be found at [Using HSM-protected encryption keys](#).

Tips for using both types of encryption

You can use both software and hardware encryption. If you choose to do so, there are some things you should be aware of.

- During a first-time install, you can configure both software and hardware encryption.
- When you install on subsequent servers, you must use the same configuration as the initial installation.
- On subsequent servers, if you only used only one form of encryption, the other encryption screen is disabled, since the system detects it is not required.

Adding software encryption to an existing system

If you install with only hardware encryption, and later go back to add software encryption, there are specific steps to follow because you will have one Venafi server with software encryption and your other servers won't be able to connect to the newly-encrypted database. Follow these steps to apply software encryption to your HSM-protected cluster:

On the first server (it doesn't matter which of your servers you pick):

1. Stop all services.
2. In Venafi Configuration Console (VCC), open **Connectors > Software > Properties** and enable **Encryption and Key Generation**.
3. Close VCC, then reopen it.

This procedure triggers the platform to generate a software key.

Export the new key, using the console, or using the following command line switch:

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

4. Restart services.

On all other servers in the cluster:

1. Stop all services.
2. Using the command line, import the key using the following command line switch:

```
tpconfiguration.exe -keyimport:<file-path>
```

For example:

```
tpconfiguration.exe -keyimport:c:\software-key.pem
```

You'll be asked to provide the password for the PEM file, then the key will be imported.

3. Restart all services.

Read more about how to use `tpconfiguration.exe` and associated command line switches at "Using the TppConfiguration command line tool" on page 99.

Installation preparation worksheet

This topic is a worksheet you can print and use to document the information required to successfully perform the base installation of Venafi Trust Protection Platform. This worksheet should be completed before you start the installation process.

Information that you gather here can be referenced during the installation process.

Venafi Platform Servers

Complete the following tables identifying your Venafi server. It is strongly recommended that a minimum of two Venafi servers be installed. Additional servers may be added at any time to accommodate for specific use-cases. Please refer to the Venafi Platform Architecture webcast at <https://ps.venafi.com> or speak to Venafi Professional Services for additional information if necessary.

Venafi Platform Server #1

FQDN Hostname of VENAFI server

Windows Server version

Server Specifications (CPU/RAM)

Venafi Platform Server #2

FQDN Hostname of VENAFI server

Windows Server version

Server Specifications (CPU/RAM)

TIP If you're installing more than two servers, make additional copies of the above tables.

Microsoft SQL Server Database

This section captures necessary information about the Microsoft SQL Database (MSSQL) that the Venafi Platform will utilize. It may be necessary to work with your organization's Database Administrator to complete this section.

Venafi Platform Database Preparation Items

MSSQL Database version

MSSQL Server FQDN Hostname

Database Name

SQL Server Instance Name (if applicable)

MSSQL Listening Port (TCP 1433 Default)

Is this an Always On Availability Group Instance?

MSSQL Server requires TLS connection?

Server Specifications (CPU/RAM)

Available Database Disk Space

Authentication Method (Windows or SQL Auth)

The database owner account is used only for installation, upgrades, and administrative maintenance.

Database Owner Account Authentication

Database AD account UPN or SQL account name

The database owner account has been granted the "DBO" role for the database.

For Windows integrated authentication:

Grant both database service accounts "Log On As a Service" permissions on all Venafi servers. For more information, see the Microsoft TechNet article [Log on as a service](#)¹.

Grant the operational database account "Log On As a Batch Job" permissions on all Venafi servers.

Add the operational database account to the local administrators group on all Venafi servers. For more information, see "Windows permissions for database service accounts" on page 64.

The operational database account is a limited account used for everyday operations. The database grants are managed automatically.

Operational Database Authentication

Database AD account UPN or SQL account name

For Windows integrated authentication:

¹<https://technet.microsoft.com/en-us/library/cc957141.aspx>

Operational Database Authentication

Grant both database service accounts "Log On As a Service" permissions on all Venafi servers. For more information, see the Microsoft TechNet article [Log on as a service](#)¹.

Grant the operational database account "Log On As a Batch Job" permissions on all Venafi servers.

Add the operational database account to the local administrators group on all Venafi servers. For more information, see "Windows permissions for database service accounts" on page 64.

HSM Storage for The Venafi Platform Encryption Key

IMPORTANT HSM connectors are global configurations. As such, the following requirements must be met before your begin:

- All Trust Protection Platform servers need to have access to the HSM.
- The HSM client must be installed to the same location on all Trust Protection Platform servers.
- The HSM client must present the same partition label on all Trust Protection Platform servers.
- Ideally the serial number presented for the partition is the same on all servers.

Make sure all of these requirements are met before creating an HSM connector.

Once these requirements are met for every Trust Protection Platform server in the cluster, you can then create a connector to the HSM from any server in the cluster.

Since HSM connectors are global configurations, each server in the cluster will load the configuration after it is created on one of them. HSM information is stored in encrypted form in the registry (only when

¹<https://technet.microsoft.com/en-us/library/cc957141.aspx>

the System Protection Key is stored in the HSM), and in Secret Store. When it is updated in VCC, the updates are stored and VCC passes the information to other servers in the cluster. If the System Protection Key is on the HSM, the individual Venafi servers will update their registries.

The HSM protected database encryption key must be accessible to all Windows servers before and after installing Venafi.

HSM Information (If Applicable)

HSM Vendor & Software Version

HSM Client Software installed version

Cryptoki DLL Path

Partition label

User Type defined

PIN - typically not required

MQTT (Message Queuing Telemetry Transport)

The Venafi Message Bus leverages MQTT to provide immediate alerts about significant changes to the database across all servers in the cluster. These alerts are informational and non-confidential, assisting servers to maintain synchronization and promptly update their configurations, permissions, and identities.

You can adjust the settings of the Message Bus and verify its status via the Venafi Configuration Console. Before you configure the firewall rules, you need to make some decisions about your MQTT setup. You have two choices:

- Self-Hosted (resembling a mesh network): If you opt for a mesh network, you need to designate a port for MQTT communication.
- Central MQTT Broker (resembling a hub-and-spoke network): If you have an existing MQTT server that you wish to use, collect the credentials and the name of your MQTT server. You will also need to designate a port for MQTT communication.

For more comprehensive information for configuring MQTT, see [Venafi Message Bus](#).

Firewall Rules

Verify your firewall rules, prepare change procedures prior to implementing the Venafi Platform. Listed below are some minimum requirements.

From	To	Port	Protocol	Purpose
Venafi Server (s)	MS SQL Server	1433	TCP	Connection to TPP database
Venafi Server (s)	DNS Server (s)	53	UDP	DNS Lookups
Venafi Server (s)	Selected AD Domain Controller (s)	UDP: 88,389 TCP: 88, 135, 389, 445, 636, 3268, 3269, 49152-65536	TCP/UDP	Required if using Active Directory Identity Provider or Windows Authentication to Database
Venafi Server (s)	LDAP Server(s)	389, 636	TCP	Required if using LDAP Identity Provider
Administrator Workstation(s)	Venafi Server(s)	3389	TCP/UDP	Access to Venafi TPP Server for administration tasks
Users	Venafi TPP UI Server(s)	443	TCP	HTTPS access to the Venafi TPP Server(s) Web UI(s) and REST API
Venafi Server (s)	Entrust nShield HSM(s)	9004	TCP	Required if using Entrust nShield HSM for encryption key

From	To	Port	Protocol	Purpose
Venafi Server (s)	LunaSA HSM(s)	1792, 22	TCP	Required if using LunaSA HSM for encryption key
Venafi Server (s)	Venafi Server(s)	Port of your choosing (8883 by default)	TCP	MQTT communication (Mesh mode). Open ports of your choosing for every Venafi Server to other Venafi Servers, e.g. incoming and outgoing.
Venafi Server (s)	MQTT Broker	Broker's required port	TCP	MQTT Communication (Central Mode). Open ports from every Venafi Server outgoing to the port the broker requires.

Preparing the database server

Trust Protection Platform requires a database to store system configuration information, archive certificates and private keys, and secure sensitive data. For database server requirements, see ["System requirements for Venafi components" on page 7](#).

Before you install Trust Protection Platform, you must do the following:

1. Create the database service accounts, create the database, and then assign the correct grants.

For more information see ["Setting up your Microsoft SQL database server" on the next page](#).

2. If you're using Windows integrated authentication, configure the necessary permissions for both database service accounts on each Venafi server.

For more information, see ["Windows permissions for database service accounts" on page 64](#).

If you plan to use Group Managed Service Accounts (gMSAs), see ["Using Group Managed Service Accounts \(gMSAs\)" on page 65](#).

Which edition of Microsoft SQL Server should I use?

When deciding which edition of Microsoft SQL Server to use with Venafi Trust Protection Platform—*Microsoft SQL Server Enterprise* or *Standard Edition*—carefully review the following table:

Use *Microsoft SQL Server Enterprise Edition* (Recommended) if you want

Automated database maintenance

Automated indexing operations

TIP The performance of index operations online is a major benefit of using Microsoft SQL Enterprise Edition. The Enterprise Edition allows the database to perform maintenance tasks automatically without requiring the database be taken offline.

Use *Microsoft SQL Server Standard Edition* if you want

Manual database maintenance

Manual indexing operations

IMPORTANT Microsoft SQL Server Standard Edition only lets you rebuild and reorganize indexes—a recommended weekly task performed manually—and requires that you take your database server offline, which results in an outage of Venafi Platform.

Support for *all three on-premise levels*:

- Level 1: Minimum requirements for up to 50k active certificates and 1k SSH servers
- Level 2: Minimum requirements for up to 250k active certificates and 5k SSH servers
- Level 3: Minimum requirements for up to 1M active certificates and 20k SSH servers

For more information about levels, see "[Locally Hosted MSSQL Requirements](#)" on page 20.

Support for *two of the three available levels*:

- Level 1: Minimum requirements for up to 50k active certificates and 1k SSH servers
- Level 2: Minimum requirements for up to 250k active certificates and 5k SSH servers

For more information about levels, see "[Locally Hosted MSSQL Requirements](#)" on page 20.

Setting up your Microsoft SQL database server

You should have a database administrator complete the following steps to set up the Trust Protection Platform database on a Microsoft SQL Server.

BEST PRACTICE Venafi recommends using two separate database service accounts for Trust Protection Platform to communicate and manage the database. The database owner account is used for installing, upgrading, and administrative maintenance. The operational database account is used for everyday operations. Having separate accounts is in line with the "Least Permissions" security principle, and is a more secure way to configure your system. The database owner account manages the necessary database grants for the operational database account.

You can connect to your database via any of the following:

- Windows integrated authentication using standard service accounts.
- Windows integrated authentication using Group Managed Service Accounts (gMSAs).
- Microsoft SQL native authentication.

Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory.

Since Windows integrated authentication is not always possible in some network segments such as DMZs, we support dual authentication, where some Venafi servers use Windows integrated authentication, while other Venafi servers connecting to the same database use MSSQL native authentication. In this scenario, you will need double the number of MSSQL service accounts.

To create the Trust Protection Platform database on a Microsoft SQL Server

1. Verify the database server meets the system requirements of your targeted deployment size of Trust Protection Platform. "[Locally Hosted MSSQL Requirements](#)" on page 20
2. Create the Trust Protection Platform database. For information on creating a database see [Microsoft's documentation on database creation](#).¹

The database name cannot contain any of the following characters:

[] () { } \ " ' , \$ % * ?

3. If you are connecting via Windows integrated authentication (including gMSAs):
 - a. Create a database owner service account and the operational database account in Active Directory.

¹<https://docs.microsoft.com/en-us/sql/relational-databases/databases/create-a-database>

- b. Grant both database service accounts "Log On As a Service" permissions on all Venafi servers. For more information, see the Microsoft TechNet article [Log on as a service](#)¹.

Grant the operational database account "Log On As a Batch Job" permissions on all Venafi servers.

Add the operational database account to the local administrators group on all Venafi servers. For more information, see "Windows permissions for database service accounts" on page 64.
 - c. Create a login for both accounts on the database server. For more information, see [Microsoft's documentation on creating logins](#).²
 - d. Grant the database owner account the DBO role to the database. For more information, see [Microsoft's documentation on granting database permissions to users and groups](#).³
4. If you are connecting to the database with MSSQL native authentication:
 - a. Create the database owner account and the operational database account on the MSSQL server. For more information, see [Microsoft's documentation on creating a database user](#).⁴
 - b. Grant the database owner account the DBO role to the database. For more information, see [Microsoft's documentation on granting database permissions to users and groups](#).⁵
5. If you are not the person installing Trust Protection Platform on the Venafi servers, provide the credential information to the person who will do the installation.

TIP If you would like information on managing and rotating your database credentials in Trust Protection Platform, see "Automatic credential rotation options" on page 110.

Permissions for enhanced performance and scalability monitoring

In large deployments where you need to closely monitor performance and scalability, you can give the operational database account additional permissions in MSSQL Server. These permissions are optional, and are only recommended if you have a dedicated SQL server for Venafi Platform, because these

¹<https://technet.microsoft.com/en-us/library/cc957141.aspx>

²<https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-login?view=sql-server-ver15>

³<https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/grant-a-permission-to-a-principal>

⁴<https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-database-user>

⁵<https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/grant-a-permission-to-a-principal>

permissions *could* give Venafi Platform the ability to query some limited details about other databases on the server.

IMPORTANT Venafi Platform **does not** collect **any** information about other databases on the server. However, because it is *possible*, we don't recommend you make these changes on shared database servers.

Granting Database Owner (DBO) permissions in Venafi is safe because Venafi is a single-user environment. In multi-user environments, DBO permissions can be risky as they allow one user to modify others' data. However, in Venafi, only Venafi services access the database, so DBO permissions don't pose a risk to other users or databases on the same SQL server.

Giving the operational database account these permissions will allow Venafi Platform administrators to have readily available performance data on the Venafi Platform database, viewable in the Venafi Statistics MMC snap-in.

Giving enhanced reporting permissions in MSSQL

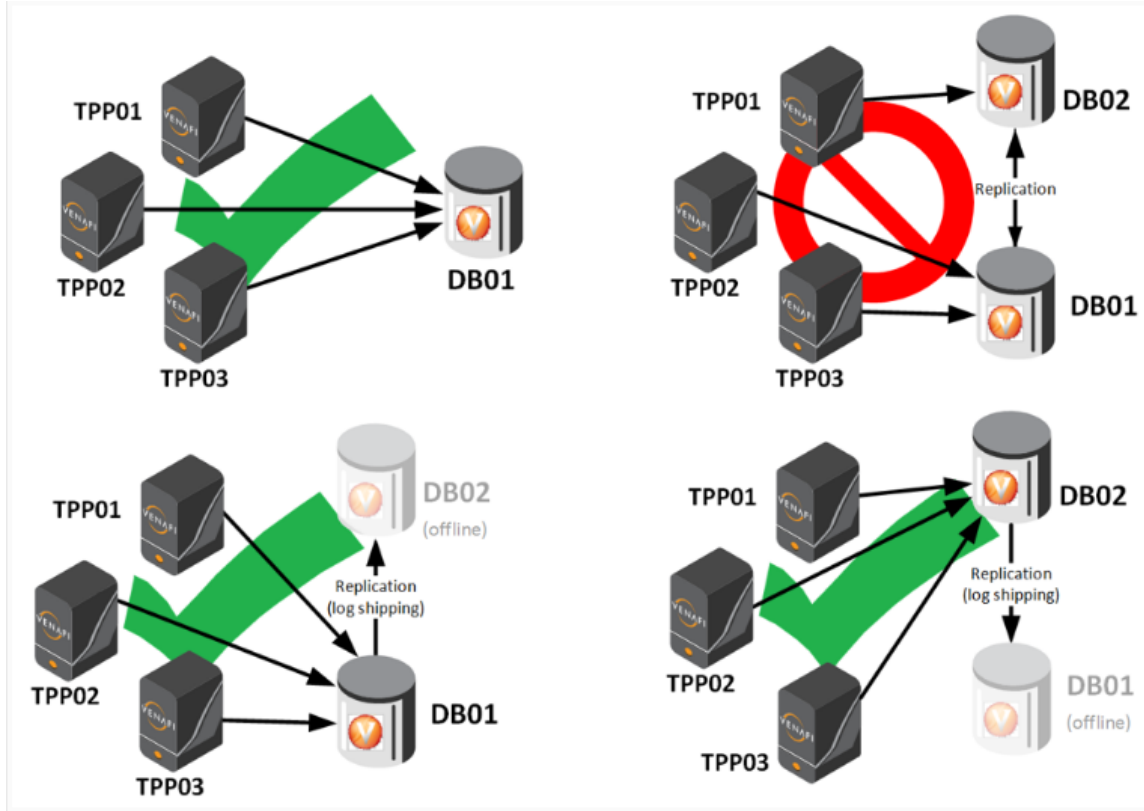
1. Log in to the database server with the database owner account.
2. In the **Object Explorer**, right-click on the database server container, then click **Properties**.
3. In the Page panel, click **Permissions**.
4. In the **Logins or roles** panel, click the name of the operational database account.
5. In the **Explicit** tab, click the **Grant** checkbox for the following permissions:
 - View any definition
 - View server state
6. Click **OK**.

AlwaysOn high-availability disaster recovery solution

Venafi supports Microsoft's MS SQL *Always On Availability Groups*. This feature is a high-availability and disaster recovery solution that provides an enterprise-level alternative to database mirroring. *Always On Availability Groups* maximizes the availability of a set of user databases for an enterprise.

IMPORTANT All Venafi Trust Protection Platform servers must connect to the **same** instance of the database.

Use of a secondary database for disaster recovery (for example, log-shipping/replication) is allowed when all Trust Protection Platform instances use a single active database.



To learn more, visit [Always On Availability Groups \(SQL Server\)](#).

For more information, visit <https://msdn.microsoft.com/en-us/library/hh510230.aspx>.

To enable this feature, see "Installing using the Venafi Configuration Console wizard" on page 67.

CAUTION Using AWS Multi-AZ (Availability Zone) requires special configuration including creating a virtual private cloud (VPC) with both private and public subnets. Please contact Venafi Customer Support for additional configuration instructions.

Windows permissions for database service accounts

When configured with Trust Protection Platform to use Windows integrated authentication to a MSSQL database, you must allocate the following permissions to the database service accounts on all Venafi servers:

Service Account	Log On as a Service	Log On as a Batch Job	Local Windows administrator group
Database owner account			
Operational database account			

With Windows integrated authentication, the Venafi Windows services and IIS application pools will be configured to launch as the operational database account. We require the security permissions "Log On As a Service" and "Log On As a Batch Job" on all Venafi servers. The Venafi installer will attempt to apply permissions automatically, if possible; however sometimes enterprise group policy domain settings prohibit us from making that change. In these cases, you will need to work with your Active Directory team to grant both database service accounts the permissions specified in the table above.

NOTE If you use the same account for both roles, that account must have all three permissions: *Log On as a Service*, *Log On as a Batch Job*, and be a member of the *Local Windows administrator group*.

For more information on the *Log On as a Service* permission, see the Microsoft TechNet article [Log on as a service](#)¹.

For more information on the *Log On as a Batch Job* permission, see the Microsoft Windows Server forum post [Log on as batch job right](#)².

You can use Group Managed Service Accounts (gMSAs) to minimize the administrative maintenance. See ["Using Group Managed Service Accounts \(gMSAs\)"](#) below.

Using Group Managed Service Accounts (gMSAs)

You can use Group Managed Service Accounts (gMSA), a type of managed domain account, for both the Database Owner account and the Operational database account.

From an operational perspective, gMSA accounts offer better security than traditional service accounts. gMSA accounts extend service account functionality over multiple servers. The domain controller and Microsoft Key Distribution Service (KDC) together manage the secrets and passwords for the devices connected with a gMSA.

¹<https://technet.microsoft.com/en-us/library/cc957141.aspx>

²<https://social.technet.microsoft.com/Forums/windowsserver/en-US/760ee186-8074-40a5-95b0-35d17c2bdfab/log-on-as-batch-job-right?forum=winserverGP>

Because of the difficulty maintaining updated passwords across devices and services, many users of standard service accounts set the password for the service account to never expire. This poses obvious security risks, and is outside policy for many organizations. Using gMSA accounts resolves this problem, so server owners and application owners don't need to worry about password rotation.

IMPORTANT Before using gMSAs with Venafi Platform, you need a good understanding of gMSA accounts, how they work, and how to administer them. In addition, you also need to have your gMSA account(s) setup and properly replicated before you can use them to configure Venafi Platform's connections to the database. The replication process can take a full business day before the gMSAs are available for use in a production environment.

Once your gMSA has been provisioned and replicated, you can use a gMSA for the database owner account as well as for the operational database account. Be sure you enter the account name in the following format:

```
<domain>\<account>$
```

For example, if my domain is `jupiter` and the gMSA account is `ganymede`, you would put the following for the user name:

```
jupiter\ganymede$
```

Don't forget the `$` at the end of the user name. If your format is correct, the password field will become disabled.

Learn more about gMSA accounts in the [Windows Server Documentation](https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview)¹.

Installing and Configuring Venafi servers

After you have created the database and created and configured the database service accounts, install and configure Trust Protection Platform. You can use either the GUI installation and configuration wizards in Windows, or you can perform a silent installation using the command prompt. Silent installations are typically used for scripting production deployments of Trust Protection Platform servers, as well as during disaster recovery procedures.

¹<https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>

IMPORTANT Make sure the servers where you install Trust Protection Platform have the required software patches and system configuration. See "[System requirements for Venafi components](#)" on [page 7](#) before proceeding.

Downloading the latest version of Venafi Trust Protection Platform

You need to download the latest version of Trust Protection Platform into your enterprise environment, and then copy the files onto your Venafi servers.

To download the latest version of Trust Protection Platform

1. Navigate to <https://community.cyberark.com/marketplace/s/#software#---Name-Trust%20Protection%20Platform~Name-Zero%20Touch%20PKI>, and log in with your CyberArk Customer Support credentials.
2. Locate the tile for the most recent version of Trust Protection Platform.
3. Click the **Components** tab.
4. Click **Download**.
5. Store the zip file(s) in your software repository, if applicable.
6. Copy the installer (and any patch) to each of the Venafi servers.

The next topic includes instructions on installing the software on the Venafi servers. You will need to repeat the steps in that topic on each Venafi server in your cluster.

Installing using the Venafi Configuration Console wizard

The Venafi Configuration Console wizard walks you through the installation of Venafi Trust Protection Platform on your server. Installation refers to both:

- Installing and connecting to a clean database
- Installing and connecting to an existing database

To Install Venafi Trust Protection Platform using the Windows installer

1. Log in to the Windows server where you want to install Trust Protection Platform.
2. Locate and extract the Trust Protection Platform zip file(s) to a staging directory.

3. From an elevated command prompt, change your directory to the extracted zip folder and enter the following command:

```
VenafiTPPInstall-25.1.x.msi
```

How to open an elevated command prompt

- a. From the Start menu, search for `CMD`.
- b. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Why do I need an elevated command prompt?

Running VenafiTPPInstall-25.1.x.msi from an elevated command prompt ensures that:

- The Venafi Configuration Console launches properly after the installation is complete.
- You can uninstall Trust Protection Platform from Windows' **Programs and Features** tool without needing to run a special command in an elevated command prompt.

4. When the Welcome window appears, click **Next**.
5. Read the terms stated in the License Agreement window. If you agree, select **I accept the terms in the license agreement**, and then click **Next**.
6. In the Destination Location window, click **Next** to accept the default location or click **Change** to change the destination folder or drive letter.

The default destination folder is:

```
C:\Program Files\Venafi\
```

7. In the **Ready to Install the Venafi Trust Protection Platform** window, click **Install** to start the installation.

The installation may take a few minutes.

NOTE Because Venafi Platform 25.1 was developed on Visual Studio 2019, it includes updated Visual Studio runtime libraries. If you have other applications running on the Windows server that also rely on the same libraries (for example, VMWare Services), you may be prompted to either 1) close those applications during installation, upgrade, or uninstallation of Venafi Platform; or 2) be prompted to restart windows at the completion of the Venafi installation process. This is expected.

If you prefer to avoid this step, you can upgrade your Visual Studio runtime libraries before you run the Venafi installer. The `vc_redist.x64.exe` libraries can be found here:

<https://support.microsoft.com/en-gb/help/2977003/the-latest-supported-visual-c-downloads>.

8. Click **Finish**.

The Windows installer completes the installation and then launches the Venafi Configuration Console wizard.

Configure Venafi platform from the Venafi Configuration Console

1. On the Venafi Configuration Console Welcome screen, determine which option applies:

- Install a new Venafi Platform Server for the first time (connect to an empty database)
- Add a Venafi Platform Server to an existing installation (connect to an existing database)

If you select this option, you will need the extracted software key from the existing installation. For information, see "[Backing up the software encryption key](#)" on page 114.

Depending on the option you choose in this step, the availability of options and the requirements for entering data will change in the following steps.

2. (Optional) If you have run this wizard previously, and you have an answer file that you want to use to pre-populate fields, select the checkbox.

For more information about working with answer files, see "[Creating and using answer files](#)" on page 89.

3. Click **Next**.

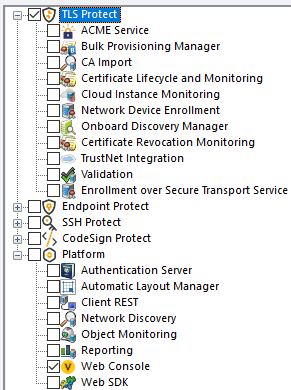
IMPORTANT On the next screen, the tabs available in the left menu depend on what options you selected on the Welcome Screen. As you continue through these steps, each of the possible tabs will be listed. If the tab doesn't appear in the Wizard, you can skip that step below. The order of the sections will also vary, depending on what you selected.

4. On the **Before You Begin** tab, read the instructions on this screen, then click **Next**.

5. [Optional] If you are using an answer file, on the **Answer File** tab click the **Browse** button to locate the answer file. If the answer file is encrypted with a password, enter the password, then click **Next**.
6. On the **Component Selection** tab, use the tree to select which components and features you want to enable for the installation.

For a list of available components, see "Trust Protection Platform components" on page 80.

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



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

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

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

Hardware encryption field descriptions

Field	Description
Name	Name of the HSM connector. This name will be how Master Admins identify this HSM connector when they are creating environment templates. In this example, we'll name it Default HSM .
Cryptoki DLL Path	Trust Protection Platform requires access to the 64-bit version of Cryptoki DLL. For SafeNet Luna SA devices, this is the path to the <code>cryptoki.dll</code> file. For Entrust nShield Connect HSM devices, this is the path to the <code>cknfast.dll</code> file. After selecting the DLL, click Load Slots. Trust Protection Platform will query the HSM and return the available slots. IMPORTANT Trust Protection Platform requires the path to the DLL file to initialize the connection to the HSM device. This path will be used for all Trust Protection Platform servers in the cluster (connected to the same database). All servers in the cluster must have their DLL file in the same location.
Slot	Slot ID for the HSM partition where you want Trust Protection Platform to access the encryption keys. NOTE While slot numbers are listed in the drop-down list, Trust Protection Platform does not depend on slot numbers. Trust Protection Platform identifies HSM partitions by label first, and in the case that there are duplicate labels, it falls back to the serial number.
User Type	User type required to access the HSM keys on the designated partition (Slot ID). The designated User Type must have sufficient permissions to use the keys in the Encryption Driver's Permitted Keys list.
Pin	Pin, if one is required to access the HSM. If you use Entrust nShield token protection, leave the field empty. If you are setting up AWS CloudHSM, the pin must be in the following format: <code><CU_user_name>:<password></code>.
Default key	The default encryption key used by the system. If you are adding a server to an existing database, you cannot change this selection. This is also the key used to protect the database connection string stored in the registry.
Create (button)	If you want to generate a new AES 256-bit symmetric key on the HSM, click this button. A new key will be generated.

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

NOTE You must select either one or both encryption types (hardware and/or software encryption). To help you decide, see ["Database Encryption"](#) on page 108.

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

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

Venafi Platform can encrypt data using a software encryption key.

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

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

Software encryption field descriptions

Field	Description
Generate a New Key	Choose this option if this is a new installation and you want the system to generate a new, unique key for this database. A random password will be generated.
Use Shared Key	Choose this option if you are connecting to an existing database secured by a software encryption key, or if you have an existing key you want to use.
Key Password	(Only if using Shared Key option) If the key is encrypted with a password, enter the key's password.
Encoded Key	(Only if using Shared Key option) Enter or paste the entire encryption key (including the --- Begin --- and ---End--- lines).

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

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

NOTE You must select either one or both encryption types (hardware and/or software encryption). To help you decide, see ["Database Encryption" on page 108](#).

IMPORTANT The keys used to encrypt Trust Protection Platform are critical to the system's functionality. Without the encryption keys you cannot access the database or stored secrets. Consequently, if you use a software encryption key, it is highly recommended that you back up the key to a secure location. In the event of a system failure, you can restore the key so Trust Protection Platform can access your system data. For information, see ["Backing up the software encryption key" on page 114](#).

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

Before you configure a new database connection, you must have previously created the Trust Protection Platform database and configured both database service accounts. For more information, see ["Preparing the database server" on page 59](#).

For information about the types of database service accounts and permissions they need, see ["Setting up your Microsoft SQL database server" on page 60](#).

Field descriptions - Settings tab

Field	Description
Hostname	Enter the hostname, FQDN, or IP address for the database connection. NOTE If you enable the TLS encrypted connection, you will need to enter the FQDN that matches the certificate presented by the MSSQL server.
Port	Enter the database port number. The default port is 1433.
Database	Enter the name for the VenafiTrust Protection Platform database.
Server supports TLS encrypted connections	Enabling this option encrypts all communications between the Venafi Platform server and the back end database. If this option is not selected, the credentials are still protected but all other communications between the server and the database might not be protected. Recommendation: Enable

Field	Description						
	To learn how to enable SSL encryption for an instance of SQL server using Microsoft Management Console, visit: https://support.microsoft.com/en-us/help/316898/how-to-enable-ssl-encryption-for-an-instance-of-sql-server-by-using-mi .						
Enable AlwaysOn Availability Groups	The Always On Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. When using this setting, use the virtual server name of the availability group listener in the hostname field. See "AlwaysOn high-availability disaster recovery solution" on page 63. For more information, visit https://msdn.microsoft.com/en-us/library/hh510230.aspx. CAUTION Using AWS Multi-AZ (Availability Zone) requires special configuration including creating a virtual private cloud (VPC) with both private and public subnets. Please contact Venafi Customer Support for additional configuration instructions.						
Database Owner Account fields	<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Type</td><td> Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords. </td></tr> <tr> <td>Login</td><td>Enter the account name that has the required permissions.</td></tr> </table>	Field	Description	Type	Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.	Login	Enter the account name that has the required permissions.
Field	Description						
Type	Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.						
Login	Enter the account name that has the required permissions.						

Field	Description						
	<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td></td><td> If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account. If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede\$</code>. Don't forget the trailing <code>\$</code>. </td></tr> <tr> <td>Password</td><td>Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.</td></tr> </table>	Field	Description		If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account. If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede\$</code>. Don't forget the trailing <code>\$</code>.	Password	Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.
Field	Description						
	If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account. If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede\$</code>. Don't forget the trailing <code>\$</code>.						
Password	Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.						
Operational Account fields	<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Type</td><td> Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords. </td></tr> <tr> <td>Login</td><td> Enter the account name that has the required permissions. If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account. </td></tr> </table>	Field	Description	Type	Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.	Login	Enter the account name that has the required permissions. If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account.
Field	Description						
Type	Trust Protection Platform allows you to use either Windows integrated authentication or Microsoft SQL native authentication to authenticate to the database. Select your connection option from the list. Windows integrated authentication is the preferred method for security purposes as it allows for central management of accounts and passwords in Active Directory. If you use gMSAs, you don't even need to worry about passwords and rotation of passwords.						
Login	Enter the account name that has the required permissions. If using Windows Authentication, enter the user name, in UPN format, of the service account user that will access the database, so that services and web applications can be configured to run under the selected account.						

Field	Description						
	<table><tr><th>Field</th><th>Description</th></tr><tr><td></td><td>If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code>. For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code>, you would use <code>jupiter\ganymede\$</code>. Don't forget the trailing <code>\$</code>.</td></tr><tr><td>Password</td><td>Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.</td></tr></table>	Field	Description		If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code> . For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code> , you would use <code>jupiter\ganymede\$</code> . Don't forget the trailing <code>\$</code> .	Password	Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.
Field	Description						
	If using a gMSA, use the format <code><DOMAIN>\<ACCOUNT>\$</code> . For example, if your domain is <code>jupiter</code> and your gMSA name is <code>ganymede</code> , you would use <code>jupiter\ganymede\$</code> . Don't forget the trailing <code>\$</code> .						
Password	Enter the password for the user account connecting to the database. If you are using a gMSA, this field will be disabled.						
NOTE The lowest level of database grants that the operational account requires is automatically provided by Trust Protection Platform through the database owner account.							
If you encounter errors during this stage, the following topics might be helpful: ◦ "Setting up your Microsoft SQL database server" on page 60, which contains information about the separate database accounts and their required roles. ◦ "Windows permissions for database service accounts" on page 64, specifically the bullet that talks about Windows integrated authentication.							

Field descriptions - Expert tab

Field	Description	
Database Owner Account	Field	Description
	Connection String	The connection string is a combination of the database settings selected above. This option is most commonly used if your database administrator instructs you to use a connection string with additional parameters that aren't available in the Venafi Configuration Console user interface.
	Password	The password to connect to the database. If there is a password provided in the connection string, that password will be used for the connection, regardless of what is set in the Password field.
Operational Account	Field	Description
	Connection String	The connection string is a combination of the database settings selected above. This option is most commonly used if your database administrator instructs you to use a connection string with additional parameters that aren't available in the Venafi Configuration Console user interface.
	Password	The password to connect to the database. If there is a password provided in the connection string, that password will be used for the connection, regardless of what is set in the Password field.

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

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

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

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

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

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

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

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

For more details on Message Bus and its configuration, see [Working with Message Bus](#).

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

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

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

For details on configuring the default algorithms, see [About default algorithm configuration](#). For a comprehensive list of supported algorithms, see [Encryption types supported by Venafi Platform](#).

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

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

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

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

Click **Next**.

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

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

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

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

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

Click **Next**.

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

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

17. Click **Finish**.

Venafi Platform will configure the server using the settings you have configured. When the configuration is complete, click **Close**.

Once you have completed the configuration wizard, the Venafi Configuration Console window automatically opens. For more information, see [Venafi Configuration Console](#) in the Administration guide.

Trust Protection Platform components

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

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

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

Component	Answer file key	Products	Description
			If this feature is installed during installation of Venafi Trust Protection Platform, it can be enabled or disabled either in the Venafi Configuration Console, or in Policy Tree on the Platforms tree. If you have multiple servers in your cluster, you may want to enable this feature on some, but not all, of the servers in the cluster for performance reasons. That would enable one server to be running the placement jobs feature without impacting the performance of other servers in the cluster.
Bulk Provisioning Manager	BulkProvisioning	TLS Protect	Provisions keys and certificates to one or more devices simultaneously.
CA Import	CAImport	TLS Protect, Client Protect	Automatically imports certificates from supported Certificate Authorities.
Certificate Lifecycle and Monitoring	Certificates	TLS Protect, Client Protect, CodeSign Protect	Provides certificate lifecycle management. Responsible for certificate-related tasks such as expiration notifications, issuance, renewal and revocation, and for provisioning of certificates to devices.

Component	Answer file key	Products	Description
Certificate Revocation Monitoring	Revocation	TLS Protect, Client Protect	Provides the ability for Trust Protection Platform to provide CRL Distribution Point monitoring. Monitors the revocation status of all certificates in inventory at least daily. Allows you to do an on-demand revocation check for an individual certificate in either Aperture or Policy Tree. Monitors OCSP and CDP endpoint validity. This component does not control your ability to revoke certificates; this component adds the ability to monitor for revocations and to monitor CDP and OCSP endpoints.

IMPORTANT Certificate Revocation and CDP Monitoring is a feature that must be enabled when you install Trust Protection Platform in the Venafi Configuration Console. This module is *disabled* by default if you are upgrading from a version of Trust Protection Platform prior to 19.2. You will need to enable it manually on at least one engine if you want to do revocation checking and CDP monitoring.

When you enable this module on multiple engines, all must have equal access to all CDP and OCSP endpoints. If a particular engine does not have the same network access as other engines, then the service module should be disabled on that engine with restricted access.

Component	Answer file key	Products	Description
			If you see sporadic network access or "unable to connect" statuses for your CDP or OCSP endpoints (either in the Roots tree, or in the logs), it is likely that one of your engines does not have access to reach those endpoints. CDP Monitoring and Revocation Checking does <i>not</i> honor engine partitioning in the Policy tree.
Client REST	Client	Platform	Enables communication between agents and Trust Protection Platform.
Code Signing Client Distribution	ClientDistribution	CodeSign Protect	Enables a web page that provides helpful scripting information and links for downloading CodeSign Protect clients. You can access the page by adding <code>/csc</code> to your Trust Protection Platform URL, such as: <code>https://TPP-Server-Name/csc</code> For more information, see Using the CodeSign Protect Client Downloads page.
Code Signing Key Server	KeyServer	CodeSign Protect	Provides functionality to set up a JWK key server and a GPG key server to store public keys and make them publicly available through a RESTful HTTP request. For more information, see GPG public key server.
Enrollment over Secure Transport Service	EstService	TLS Protect, Client Protect	This service provides certificate enrollment capability for devices via the Enrollment over Secure Transport (EST) protocol.

Component	Answer file key	Products	Description
			For more information on EST, see Certificate enrollment via EST protocol .
HSM Backend	HsmBackend	CodeSign Protect	Provides virtual HSM capability within Trust Protection Platform for code signing. This allows Venafi CodeSign Protect clients to request signing operations using private code signing keys that are managed by Trust Protection Platform.
Key Lifecycle and Monitoring	KeyManager	CodeSign Protect	Provides key lifecycle management. Responsible for tasks such creating new keys and monitoring key expiration. This component is required for GPG and .NET CodeSign Protect Environments, as well as for SSH Protect.
Kubernetes Discovery Manager	JSSDiscovery	TLS Protect	Provides a way to monitor TLS certificates used on clusters managed by Venafi TLS Protect for Kubernetes. With the Kubernetes discovery feature, administrators can create new discovery jobs which import certificates from all Kubernetes clusters registered to Venafi TLS Protect for Kubernetes.
Network Device Enrollment	Scep	TLS Protect, Client Protect	Enables devices to use the SCEP protocol to request certificates from Trust Protection Platform.

Component	Answer file key	Products	Description
			You would want to enable this feature if you have SCEP-enabled devices or applications and you want those devices and applications to be able to get certificates directly from Trust Protection Platform. This feature is frequently used with mobile-device management solutions. For more information on configuring Network Device Enrollment, see Managing network device enrollment (NDE) of the <i>Venafi Trust Protection Platform Certificate Management Guide</i>.
Network Discovery	Discovery	Platform	Runs the Network Discovery surveys configured in your system's Discovery objects. During a Network Discovery, the Discovery server scans designated IPv4 address ranges and ports to identify SSL certificates. For more information on discovering network certificates, see Discovering certificates and keys in the Venafi Administration Guide.
Object Monitoring	Monitoring	Platform	Monitors SSH key and credential objects for expiration and generates expiration notifications. For more information on logging and event notifications, see Notification and logging overview in the <i>Venafi Trust Protection Platform Administration Guide</i>.

Component	Answer file key	Products	Description
Onboard Discovery Manager	OBDDiscovery	TLS Protect	Configuring onboard discovery jobs lets you automate the process of provisioning by adding devices to one or more specific policies. You then have control over the placement of discovered certificates without having to manually update jobs or reorganize certificates after they've been discovered.
Reporting	Reporting	Platform	Generates and distributes pre-defined and custom reports.
SSH Certificate Lifecycle and Monitoring	SSHCertificates	SSH Protect	Allow you to use SSH Protect to manage SSH Certificates.
SSH Key Detection and Remediation	SSH	SSH Protect	Secures and protect SSH keys and systems through discovery, reporting, policy enforcement, and remediation.
Time Stamp Service	TimeStampService	CodeSign Protect	Provides an RFC 3161-compliant time stamping service for code signing. This service allows you to use either your own time stamping certificate or to specify a list of time stamping proxies. Once configured, you can then specify Trust Protection Platform as your time stamping server.
Validation	Validation	TLS Protect, Client Protect	Runs the network and onboard validation processes. Network validation verifies a certificate or key is installed on the target system, then determines if the correct certificate is being used.

Component	Answer file key	Products	Description
			For more information on validating certificates and applications, see SSL/TLS network validation of the <i>Venafi Trust Protection Platform Certificate Management Guide</i> .
Web Console	WebConsole	Platform	Web-based management interface. Installs both Policy Tree and Aperture. At least two Venafi servers needs to have Web Console enabled. If Web Console is configured on two different servers, you can disable this component. Server requirements for Web Console are outlined in "Web Server Roles (Venafi web services enabled)" on page 11.
Web SDK	WebSDK	Platform	Extend your custom environments by integrating them with Venafi solutions using the Venafi Web SDK code library. For more information, see About this guide in the <i>Trust Protection Platform Developer's Guide</i>.

Command line installation and configuration

You don't need to use the GUI configuration wizard to install or upgrade Trust Protection Platform. The platform includes a utility that allows you to work directly from the command line, and more importantly, allows you to script installation and configuration for a Venafi Trust Protection Platform server.

Our documentation is in the context of the silent/unattended installation. It will use batch files as a reference implementation, but can be used with any scripting language.

This chapter shows you how to use the command-line utility to install and configure Trust Protection Platform either directly, or via a script (like a batch file).

The general steps for using the command-line utility are listed below. More details about each step can be found via the link provided.

1. First, download the latest version of Trust Protection Platform as well as any applicable patch. For more information see ["Downloading the latest version of Venafi Trust Protection Platform" below](#).
2. Create an answer file for configuring the platform settings. For more information see ["Creating and using answer files" on the facing page](#).
3. Create a script for installation and configuration, then add the commands for installing `VenafiTPPInstall-25.1.x.msi`. For more information see ["Install the MSI file from the command line" on page 96](#).
4. Update your installation and configuration script to leverage the `TapConfiguration.exe` utility with your answer file and appropriate switches. For more information see ["Configure the platform using a script through the command line" on page 97](#).
5. Run your installation and configuration script. For more information see ["Run script and review response codes" on page 106](#).
6. Repeat this process on each Venafi server in your deployment.

Downloading the latest version of Venafi Trust Protection Platform

You need to download the latest version of Trust Protection Platform into your enterprise environment, and then copy the files onto your Venafi servers.

To download the latest version of Trust Protection Platform

1. Navigate to <https://community.cyberark.com/marketplace/s/#software#---Name-Trust%20Protection%20Platform~Name-Zero%20Touch%20PKI>, and log in with your CyberArk Customer Support credentials.
2. Locate the tile for the most recent version of Trust Protection Platform.
3. Click the **Components** tab.
4. Click **Download**.

5. Store the zip file(s) in your software repository, if applicable.
6. Copy the installer (and any patch) to each of the Venafi servers.

The next topic includes instructions on installing the software on the Venafi servers. You will need to repeat the steps in that topic on each Venafi server in your cluster.

Creating and using answer files

An answer file is an XML file that contains pre-determined configuration settings. You have an option to create an answer file at the end of the Venafi Platform Configuration wizard. Once you have an answer file, you can use it to specify configuration settings, making it much faster to deploy future Venafi Trust Protection Platform installations.

You can create an answer file without deploying the software by checking the appropriate option on the Configure Server tab of the Venafi Platform configuration wizard.

Below is a sample unencrypted answer file. You can use this sample file and modify it for your specific needs, as long as you are willing to use an unencrypted file. If you prefer to use an encrypted answer file, you need to generate it from the Venafi Platform configuration wizard. An unencrypted answer file is a plain text XML file that contains information like your master admin user name and password, your database connection credentials, your software encryption key, and all other configuration settings. You can read [more information about creating and encrypting answer files via the configuration wizard](#).

Answer file sections and settings

Products section

You need to include the products that are linked to each of the features enabled in the Features section. To see how features map to products, see ["Trust Protection Platform components" on page 80](#).

For example, If you only specify the `WebConsole` feature, you only need the `CommonProduct` product.

You can only install products for which you have a license.

Decide what features you want, using the components page.

Reference the components page to determine what products are necessary for the features you want.

- `TLSProtectProduct` is called **TLS Protect** on the components page.
- `ClientProtectProduct` is called **Client Protect** on the components page.

- `SSHProtectProduct` is called **SSH Protect** on the components page.
- `CodeSignProtectProduct` is called **CodeSign Protect** on the components page.
- `PlatformProduct` is called **Platform** on the components page.

Features section

For the `<Features>` section, information on each feature name and what it provides is described in "Trust Protection Platform components" on page 80.

DSN sections

For the `<DSN>` sections for both `<DBO>` and `<Database>` entries, information on how DSNs (Data Source Name) are constructed is found in Microsoft's documentation, [Connection Options](#)¹.

The `TrustServerCertificate` option, if set to true, means we will encrypt the connection and validate the certificate.

The `MultiSubnetFailover` option, if set to true, enables always on availability groups.

The `Integrated Security` option, if included, enables Windows integrated authentication. If this value is missing, the system will use MSSQL database authentication.

The `Data Source` option is the database address and port

The `Initial Catalog` option is the name of the database

Hardware encryption section

For new installations: you must choose one of the following options:

- Hardware encryption
- Software encryption
- Both hardware encryption and software encryption

¹<https://docs.microsoft.com/en-us/sql/connect/php/connection-options?view=sql-server-ver15>

For additional servers, this section needs to match the section on all other Venafi servers. If you are not using an HSM for hardware encryption, then the entire `<HardwareEncryption>` section will not be present.

Software Encryption section

If you want the system to generate a new software encryption key, you can leave out this element. If you have a key from another system that you want to use, you can enter it this way: If you want to use software encryption to protect data in the Trust Protection Platform database, you need to configure the software encryption element.

Using existing software encryption key

```
1 <!-- Use the following SoftwareEncryption element to use a previously-
   generated software key on additional servers. If you want the system to
   generate a new key, omit this element. -->
2 <SoftwareEncryption>
3     <Key>-----BEGIN VED ENCRYPTED KEY-----
4         <!-- Base64 Encrypted key text -->
5     -----END VED ENCRYPTED KEY-----</Key>
6     <Password>ExamplePassword</Password>
7 </SoftwareEncryption>
```

Admin Account

The AdminAccount section is where you provide the username and password for the local master administrator account for Trust Protection Platform. If you have already created this on another Venafi server, this must match that setting. If this is your first Venafi server, this will establish that account. Password requirement complexity is documented in [Changing local user passwords](#).

Message Bus

The MessageBus section is where you provide configuration information for using the MQTT message broker service we call Message Bus. Additional information about Message Bus can be found in [Working with Message Bus](#).

Available Algorithms

The Available Algorithms section defines which algorithms are programmatically allowed by Venafi Platform. Additional information about algorithms can be found in [About default algorithm configuration](#).

Server section

The `StartServices` option, if set to yes, will automatically start Venafi services on the Venafi server after the configuration is complete.

On your first Venafi Platform server, you don't want to start services automatically, since there are still configuration steps you want to do first. However, if you are creating an answer file for second (or subsequent) servers, this switch can save some manual steps on each server.

If you are setting this server up as a log server, there will be a `LogPath` option with the file path where the log data will be saved.

Complete answer file example

The following is a complete answer file with all possible options enabled. You can use this as a starting point for your answer file, or you can generate one from the Venafi Configuration Console. Your final answer file will likely be shorter, as you are unlikely to enable every option on all Venafi servers.

```
1  <?xml version="1.0" encoding="utf-8" standalone="yes"?>
2      <TppConfiguration CreatedOn="12/31/2025
3          12:00:00" By="abe.lincoln" On="WIN-Venafi01">
4          <Components>
5              <Products>
6                  TLSProtectProduct
7                  ClientProtectProduct
8                  SSHProtectProduct
9                  CodeSignProtectProduct
10                 PlatformProduct
11             </Products>
12             <Features>
13                 Acme
14                 BulkProvisioning
```

```
14         CAImport
15         Certificates
16         Scep
17         OBDDiscovery
18         JSSDiscovery
19         Revocation
20         Validation
21         EstService
22         SSH
23         SSHCertificates
24         HsmBackend
25         TimeStampService
26         KeyManager
27         KeyServer
28         ClientDistribution
29         AuthServer
30         AutoLayout
31         Client
32         Discovery
33         Monitoring
34         Reporting
35         WebConsole
36         WebSDK
37     </Features>
38 </Components>
39 <DBO>
40     <DSN>Data Source=mssql.example.com,1433;Initial Catalog=VenafiDB; User
ID=DBO_user@example.com;Password=ExamplePassword;
TrustServerCertificate=True;MultiSubnetFailover=True;Integrated
Security=True</DSN>
```

```

41     </DBO>
42     <Database>
43         <DSN>Data Source=mssql.example.com,1433;Initial Catalog=VenafiDB; User
ID=Operational_user@example.com;Password=ExamplePassword;
TrustServerCertificate=True;MultiSubnetFailover=True; Integrated
Security=True</DSN>
44     </Database>
45     <HardwareEncryption>
46         <DllPath>c:\program files\myhsmvendor\pkcs11library.dll</DllPath>
47         <Slot>0</Slot>
48         <Pin>ExamplePassword</Pin>
49         <Key>MyDemoKey</Key>
50         <AccountType>CryptoOfficer</AccountType>
51     </HardwareEncryption>
52     <!-- Use the following SoftwareEncryption element to use a previously-
generated software key on additional servers. If you want the system to
generate a key, omit this element. -->
53     <SoftwareEncryption>
54         <Key>-----BEGIN VED ENCRYPTED KEY-----
55         <!-- Base64 Encrypted key text -->
56         -----END VED ENCRYPTED KEY-----</Key>
57         <Password>ExamplePassword</Password>
58     </SoftwareEncryption>
59     <AdminAccount>
60         <Username>masterAdmin</Username>
61         <Password>ExamplePassword</Password>
62     </AdminAccount>
63     <!-- This Message Bus element is for a mesh connection. Use either this
one OR the hub and spoke connection, not both. -->
64     <MessageBus>
65         <Port>8883</Port>

```

```

66         <!-- 8883 is recommended for TLS encrypted. Port 1883 is recommended
for unencrypted. -->
67         <Tls>yes</Tls>
68         <!-- Use 'no' for unencrypted -->
69     </MessageBus>
70     <!-- This Message Bus element is for hub and spoke connection to a central
broker. Use either this one OR the mesh connection, not both. -->
71     <MessageBus>
72         <Port>8883</Port>
73         <!-- 8883 is recommended for TLS encrypted. Port 1883 is recommended
for unencrypted. -->
74         <Tls>yes</Tls>
75         <!-- Use 'no' for unencrypted -->
76         <Server>name</Server> <!-- Central server -->
77         <Instance>id</Instance> <!-- Central instance id -->
78         <Username>name</Username> <!-- Central auth username; if auth required
-->
79         <Password>password</Password> <!-- Central auth password; if auth
required -->
80         <Certificate>PFX data</Certificate> <!-- Central auth certificate; in
lieu of username/password -->
81     </MessageBus>
82     <AvailableAlgorithms>
83         1.3.6.1.4.1.28783.10.5.1.6
84         1.3.6.1.4.1.28783.10.7.15
85         1.3.6.1.4.1.28783.10.7.14
86         1.3.6.1.4.1.28783.10.7.13
87         1.3.6.1.4.1.28783.10.2.2.14
88         1.3.6.1.4.1.28783.10.5.1.12
89         1.3.6.1.4.1.28783.10.5.2.11
90         1.3.6.1.4.1.28783.10.5.2.6

```

```
91      <!-- Other algorithms would normally be listed but are truncated here
for length. -->
92      </AvailableAlgorithms>
93      <Logging>
94          <LogProcessor />
95          <LogExpiration Days="90" />
96      </Logging>
97      <Environment>
98          <CompanyName>Example Company, Inc.</CompanyName>
99          <DeploymentType>PRODUCTION</DeploymentType>
100     </Environment>
101     <Server>
102         <StartServices>yes</StartServices>
103         <LogPath>C:\Program Files\Venafi\Logs\Tpp Configuration
Log.txt</LogPath>
104     </Server>
105 </TppConfiguration>
```

Install the MSI file from the command line

The first step in using the command line installation utility is to copy the MSI file to your Venafi Trust Protection Platform server, and run it using the following procedure.

To install Trust Protection Platform using the command line

1. Log in to the Windows server where you want to install Trust Protection Platform.
2. Locate and extract the Trust Protection Platform zip file(s) to a staging directory.
3. Use a text editor to create a batch file (*.bat).
4. Inside the batch file, add the following command:

```
Echo Installing Venafi Trust Protection Platform
```

```
msiexec /i "[Staging_Directory]\Product\ VenafiTPPInstall-25.1.x.msi" /q /n
```

In the previous command, the `x` represents the "dot version." Refer to your download package and use the correct filename you downloaded.

NOTE To enable logging during install, add `/L*VX` then the path to the logging file. For example:

```
msiexec /i "[Staging_Directory]\Product\VenafiTPPInstall- 25.1.0.msi" /q /n /l*vx "[Full file path]\install.log"
```

To specify a custom installation folder, use the `INSTALLDIR` switch. For example:

```
msiexec /i "[Staging_Directory]\Product\VenafiTPPInstall-25.1.x.msi" /q /n INSTALLDIR="[e:\Program Files\Venafi]"
```

For more information on the switches you can use during installation see Microsoft's documentation on [How to enable Windows Installer logging](#)¹.

In the next topic, you will add the necessary commands to configure the platform in your script.

Configure the platform using a script through the command line

The next step for scripting a command-line installation and configuration is to add the command to the script to configure the platform's settings. You can use the script file you started creating in "Install the MSI file from the command line" on the previous page.

Configuring the platform from the command line requires you have an XML answer file that contains the product and feature information for each specific Venafi server. For more information on answer files, see "Creating and using answer files" on page 89.

To script the configuration for the first Venafi server with an empty database

NOTE Only use this step the first time you install Venafi Trust Protection Platform against a new database.

¹<https://support.microsoft.com/en-us/help/223300/how-to-enable-windows-installer-logging>

- Using your text editor to edit the batch file, add the following command:

```
"[installation directory]\Venafi\Platform\TppConfiguration.exe" -install:"[path to answer file]" -password:[encrypted answer file password]
```

For example, to install Trust Protection Platform as a first-time installation from the default installation directory using a previously-created answer file located in

`c:\WebServicesAnswerFile.xml`, you would use the following command:

```
Echo Configuring Venafi Trust Protection Platform  
"c:\Program Files\Venafi\Platform\TppConfiguration.exe" -install:"C:\WebServicesAnswerFile.xml" -password:ExamplePassword
```

To script the configuration for all additional servers with an existing database

If this is only a two-server deployment, you will use need to export the software encryption key from the first server (see "Backing up the software encryption key" on page 114), add that key to the answer file, and then use the new answer file on the second server.

If you are using three or more Venafi servers, you will need a custom answer file for each server type (web services, Logging event processing, back-end processing servers, or agent processing).

When scripting for second, third, or more servers you use the `-add` switch at the end of the installation command.

- Using your text editor to edit the batch file, add the following command:

```
"[installation directory]\Venafi\Platform\TppConfiguration.exe" -install:"[path to answer file]" -password:[encrypted answer file password] -add
```

For example, to install Trust Protection Platform as a first-time installation from the default installation directory using a previously-created answer file located in `c:\Back-`

`EndProcessingAnswerFile.xml`, you would use the following command:

```
Echo Configuring Venafi Trust Protection Platform  
"c:\Program Files\Venafi\Platform\TppConfiguration.exe" -install:"C:\Back-EndProcessingAnswerFile.xml" -password:ExamplePassword -add
```

For a comprehensive list of command line switches for `TppConfiguration.exe`, see "Using the TppConfiguration command line tool" on the facing page.

Using the TppConfiguration command line tool

Venafi Platform includes a command-line utility that allows system admins to perform installation and configuration actions through the command line or through script files. It provides administrators with greater flexibility and automation capabilities when managing the platform, especially when dealing with multiple environments or large-scale deployments.

The utility is called TppConfiguration.exe and exists in the installation directory, in the following location (assuming you used the default installation directory):

```
C:\Program Files\Venafi\Platform\TppConfiguration.exe
```

This utility requires you to use an elevated command prompt.

How to open an elevated command prompt

1. From the Start menu, search for `CMD`.
2. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Using the TppConfiguration command, administrators can:

- Script the installation or upgrade of Venafi Platform on servers.
- Update the database connection information for a Venafi Platform server.
- Enable access to the MMC snapins for the current Windows user.
- Update the company name or installation type of a server.
- Uninstall Venafi Platform.
- Update the HSM pin.

When using the command line utility to install, configure, upgrade, or uninstall Trust Protection Platform, there are a number of allowed switches. This utility requires you to use an elevated command prompt.

The command line argument is:

```
TppConfiguration.exe -<switch>=<value> -<switch2>=<value>
```

Some switches require master admin authentication. They are noted in the table below. When you use a switch that requires master admin authentication, you can either:

- Provide the `-username` and `-password` inline in the command. (Required if you are scripting the command.)
- Wait until prompted by the application to enter the master admin credentials.

TPPConfiguration syntax

- The command line tool uses a flexible syntax. Simply run the `TPPConfiguration` program with parameters to perform specific tasks.

For example, `TPPConfiguration -errorcodes` will output a list of return codes and a description of the error. Neither commands or parameters are case sensitive, meaning `tppconfiguration -errorcodes` and `TPPConfiguration -errorcodes` and `TPPCONFIGURATION -ERRORCODES` are all interpreted the same.

- To perform specific tasks, type a parameter directly after typing the `TPPConfiguration` command. For instance, `TPPConfiguration -enablemmc`.
- When running the program with no parameters, you will see the inline help. There, you will see that some characters in parameter names are bolded and some are not. The bolded characters are a short-cut syntax that makes it quicker and easier to type commands. For example, the `add` parameter is displayed in the inline help as `-add`. The bolded part, in this case `-a`, is the short cut.

This short-cut syntax can make it quicker and easier to type commands; however, to ensure compatibility with future versions of TPPConfiguration, you should use full parameter names when scripting.

TIP The hyphen (`-`) is technically optional, but is recommended for forwards compatibility.

- Command options are additional modifiers that provide further instructions or information to the TPPConfiguration command being executed. For example, `-username=<master-admin-user>` is used to indicate the username of the master administrator account needed to perform the action. The tool accepts the following operators: `=`, `:`, and (space). Thus the following examples are all treated the same: `-username=venafi`, `-username:venafi`, and `-username venafi`

Combining these principles, the following commands are all interpreted the same:

```
TPPConfiguration -enablemmc -username=george.washington -password=Passw0rd!11
```

```
tppconfiguration enablemmc username george.washington -password Passw0rd!11
```

```

TppConfiguration.exe -ENABLEMMC -username:george.washington
pa:Passw0rd!11

```

```

tppconfiguration ena us:george.washington pa Passw0rd!11

```

Configuration switches for TppConfiguration.exe command line tool

Click a column header to sort by that column.

Parameter	Type	Auth ¹	Description
<code>-errorcodes</code> <code>-er</code>	Common Options	No	Show all error codes that may be returned.
<code>-password:<pw></code> <code>-pa:<pw></code>	Common Options	Yes	Password to decrypt the answer file.
<code>-username=<name></code> <code>-us=<name></code>	Common Options	No	User name of local Venafi Platform admin account.
<code>-keyexport=<pem></code> <code>-keye=<pem></code>	Configuraiton	Yes	Exports the default software key. (Requires <code>-password</code>)
<code>-dboconfig=<cfg></code> <code>-dbo=<cfg></code>	Configuration	No	Allows changing the SQL database owner account connection information from the command line. You can use this, for example, for automated updating of the SQL database owner account password. For details on the connection string and its proper syntax, see Obtaining the SQL database connection string .

¹Shows if the parameter requires authentication. If yes, pass using the `-username` and `-password` parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth ¹	Description
<code>-keyimport=<pem></code> <code>-keyi=<pem></code>	Configuration	Yes	Imports the default software key. (Requires <code>-password</code>)
<code>-sqlconfig:<cfg></code> <code>-s:<cfg></code>	Configuration	No	Allows changing the SQL operational account connection information from the command line. You can use this, for example, for automated updating of the SQL operational account password. For details on the connection string and its proper syntax, see Obtaining the SQL database connection string .
<code>-add</code> <code>-a</code>	Installation	No	Runs the installer in the mode that adds this Venafi server to an existing Venafi server cluster (servers that share a single database).
<code>-install=<xml> -password=<pw></code> <code>-in=<xml> -pa=<pw></code>	Installation	No	Runs the installer (fresh install if DB is empty; upgrade if DB is not empty) with the configuration options specified in the answer file, and supplies the password to decrypt the answer file. For example, if the answer file is located at <code>c:\answerfile.xml</code> and the decryption password for the file is <code>Example"Password</code> , this switch would be:

¹Shows if the parameter requires authentication. If yes, pass using the `-username` and `-password` parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth ¹	Description
<code>-install:C:\answerfile.xml</code> <code>-password:Example\"Password</code>			NOTE The quotation mark " and backslash \ characters are special characters, and if included in the password, you need to include a backslash to escape them. So if the password is pas"sw\ord, you would enter it as pas\"sw\ord.
<code>-log=<file></code> <code>-l=<file></code>	Installation	No	Allows you to override the default location of the log file where the results of the configuration process are stored. If you want to save the log file at C:\Temp\VenafiLog.txt, the switch would be: <code>-log:C:\Temp\VenafiLog.txt</code>
<code>-uninstall</code> <code>-un</code>	Installation	No	Uninstalls Trust Protection Platform from the Venafi server by doing the following: Removes Venafi registry values, and backs up settings to a registry file stored in the same folder as the log file.

¹Shows if the parameter requires authentication. If yes, pass using the `-username` and `-password` parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth ¹	Description
			Removes the Venafi website from IIS. This switch is used by Windows when you use Program Features to uninstall Trust Protection Platform. NOTE This does not remove the files or Windows Services installed by the .msi. It only removes the websites and registry entries.
<code>-company=<name></code>	Miscellaneous	Yes	Sets the company name for the system.
<code>-c=<name></code>			
<code>-decrypt=<xml></code>	Miscellaneous	Yes	Decrypts the specified XML file. (Requires <code>-password</code>)
<code>-dec=<xml></code>			
<code>-deployment=<t></code>	Miscellaneous	Yes	Sets the deployment type for the system. Allowed values for <code><t></code> are:
<code>-dep=<t></code>			<code>D</code> - Development <code>T</code> - Test <code>S</code> - Staging (pre-production) <code>U</code> - User Acceptance Test (UAT) <code>P</code> - Production
<code>-encrypt=<xml></code>	Miscellaneous	Yes	Encrypts the specified XML file. (Requires <code>-password</code>)

¹Shows if the parameter requires authentication. If yes, pass using the `-username` and `-password` parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth ¹	Description
<code>-enc=<xml></code>			
<code>-help</code>	Miscellaneous	No	Shows a help file in the command line window, describing these features and settings.
<code>-</code>			
<code>-dbgrant=<user></code>	Recovery	Yes	Provides the necessary grants to the Venafi database for the specified user to be an operational database service accounts. This is helpful when using Windows Authentication and users need to launch WebAdmin or Venafi Support Tool.
<code>-dbg=<user></code>			
<code>-driverpwd=<new-pw></code>	Recovery	Yes	Requests to change the service account password of an identity connector. <code><new-pw></code> is the new password. Uses <code>-name</code> , <code>-username</code> , and <code>-password</code> and will prompt if any are omitted.
<code>-dr=<new-pw></code>			
<code>-enablemmc</code>	Recovery	Yes	Adds or replaces MMC access grant for the current user. Use <code>-username:</code> and <code>-password:</code> to provide Trust Protection Platform user credentials on the command line. Otherwise, you will be prompted for credentials.
<code>-ena</code>			
<code>-hsmpin=<pin></code>	Recovery	No	Allows setting the HSM PIN in an HSM-only environment. This is necessary if the HSM pin has been changed, and needs to be updated in Trust Protection Platform.
<code>-hs=<pin></code>			

¹Shows if the parameter requires authentication. If yes, pass using the `-username` and `-password` parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Parameter	Type	Auth ¹	Description
			Note: When used without the <pin> argument, you will be prompted for the pin.
-name=<cn> -n=<cn>	Recovery	Yes	The common name of an identity connector object.
-distrust=<dll> -di=<dll>	Trust	No	Allows you to remove a DLL from being a trusted resource.
-trust=<dll> -tr=<dll>	Trust	No	The path to a custom DLL, allowing it to be added as a trusted resource. For custom development modules, this feature adds the signature of the custom module as trusted resource so the custom features can be added to Trust Protection Platform.

You can combine the switches as needed. For example, here is a command line argument that installs the software on this Venafi Trust Protection Platform server, while connecting to an existing database using a configuration file, and overwriting the default log file location:

```

TppConfiguration.exe -in=C:\answerfile.xml -add -pa=Washington -
l=C:\Temp\VenafiLog.txt

```

Run script and review response codes

Now that your batch file contains the necessary commands to install and configure Trust Protection Platform, you're ready to run the script (with elevated privileges) on each Venafi server. For example, with the batch file created in the previous sections, you could right-click on the file and select **Run as Administrator**.

¹Shows if the parameter requires authentication. If yes, pass using the **-username** and **-password** parameters when scripting, or, if running manually, you can omit, and the utility will prompt you for your admin credential.

Response codes

When running the command line configuration utility, you will get one of the following response codes after the configuration script runs. This list provides the response codes and a description of what the response code means, as well as the action you should take to remedy the situation.

Code	Description	Additional Information
0	The Trust Protection Platform configuration completed successfully	
1	The specified XML file could not be opened, or does not exist	Check the spelling and directory information to ensure the file is in the specified location.
2	An error occurred trying to process the XML file	The XML answer file's password might be incorrect, or the XML file contains invalid syntax, or contains unexpected properties or values.
3	The installation process failed	
4	The system could not detect the installation mode	
5	The system is already up to date with the latest code.	No action was taken. If this is unexpected, verify that you have the latest version of Venafisoftware.
6	TppConfiguration.exe was called without administrator rights.	Your command prompt must have administrative permissions to complete this action. Run the command prompt as an administrator.
100	TppConfiguration.exe encountered an unexpected failure (exception)	Error details are written to the log file. Review the details and, if necessary, contact Venafi Support.

Code	Description	Additional Information
200	TppConfiguration.exe failed to add a third-party trusted signer.	
201	TppConfiguration.exe failed to remove a third-party trusted signer.	
202	TppConfiguration.exe failed to read the third-party DLL.	

Database Encryption

Venafi Platform uses encryption at rest to protect the information stored in your database. There are two options for database encryption: software encryption, and hardware encryption. You must use some combination of the two (hardware, or software, or both).

Understanding your encryption options is important so you know how Venafi Platform is protecting your data.

For more information on encryption drivers and how to configure them, see [Overview of encryption drivers](#).

Software Encryption

If you select software encryption, your database assets will be encrypted using an AES-256 encryption key stored in the Windows registry. You either provide a key, or have Venafi Platform generate a key for you. You must use the same encryption key on all Venafi servers.

To export your software key for backup or to use on another server, you can use the Venafi Configuration Console (VCC), or you can use the command line.

For information on using VCC, see ["Backing up the software encryption key" on page 114](#).

To backup using the command line, run the following command:

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

Hardware Encryption

If you select hardware encryption, your encryption material will be stored on a hardware security module (HSM), such as one provided by SafeNet Luna SA, Entrust nShield, or other HSM provider.

NOTE While most other uses of HSMs require Venafi Advanced Key Protect (AKP), you can encrypt secrets in your database using an HSM without a license for AKP.

More information on hardware encryption can be found at [Using HSM-protected encryption keys](#).

Tips for using both types of encryption

You can use both software and hardware encryption. If you choose to do so, there are some things you should be aware of.

- During a first-time install, you can configure both software and hardware encryption.
- When you install on subsequent servers, you must use the same configuration as the initial installation.
- On subsequent servers, if you only used only one form of encryption, the other encryption screen is disabled, since the system detects it is not required.

Adding software encryption to an existing system

If you install with only hardware encryption, and later go back to add software encryption, there are specific steps to follow because you will have one Venafi server with software encryption and your other servers won't be able to connect to the newly-encrypted database. Follow these steps to apply software encryption to your HSM-protected cluster:

On the first server (it doesn't matter which of your servers you pick):

1. Stop all services.
2. In Venafi Configuration Console (VCC), open **Connectors > Software > Properties** and enable **Encryption and Key Generation**.
3. Close VCC, then reopen it.

This procedure triggers the platform to generate a software key.

Export the new key, using the console, or using the following command line switch:

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

4. Restart services.

On all other servers in the cluster:

1. Stop all services.
2. Using the command line, import the key using the following command line switch:

```
tpconfiguration.exe -keyimport:<file-path>
```

For example:

```
tpconfiguration.exe -keyimport:c:\software-key.pem
```

You'll be asked to provide the password for the PEM file, then the key will be imported.

3. Restart all services.

Read more about how to use `tpconfiguration.exe` and associated command line switches at ["Using the TppConfiguration command line tool" on page 99](#).

Automatic credential rotation options

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

Credentials you can script for rotation:

- HSM connection pin
- Trust Protection Platform database connection password
- Identity provider. For more information, see [Updating an identity provider connection password](#).

To reset the HSM connection pin using the command line

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

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

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

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

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

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

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

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

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

For more information on using the command line to perform actions in Trust Protection Platform, see "Configure the platform using a script through the command line" on page 97 in the Installation and Upgrade Guide.

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

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

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

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

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

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

For example:

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

To obtain your current SQL configuration string, see [Obtain SQL database connection string in the Administration Guide](#).

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

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

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

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

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

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

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

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

For example:

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

To obtain your current SQL configuration string, see [Obtain SQL database connection string in the Administration Guide](#).

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

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

For more information about the TPPConfiguration utility, see ["Using the TppConfiguration command line tool" on page 99](#).

Post-installation procedures

This chapter documents how to start Venafi Trust Protection Platform™ and other post-installation procedures.

Starting Venafi Trust Protection Platform services

When you complete the Trust Protection Platform installation, you must reboot your server *or* manually start Venafi Trust Protection Platform and Venafi Log Server services.

NOTE When you reboot your server after installation, the Venafi Log server and Venafi Trust Protection Platform services start automatically.

You can start (and stop) Venafi services using the Venafi Configuration Console (VCC).

The Venafi Log Server service provides logging and notification services. The Venafi Trust Protection Platform service loads all service modules and provides a framework for managing, monitoring, and validation.

To start Venafi Trust Protection Platform services manually using VCC

1. On the application server where you've installed Trust Protection Platform, open **VCC**.
2. In the left panel, click the **Product** node.
3. In the center panel, right-click on **Venafi Platform** and click **Start**.
4. Right-click on **Logging** and click **Start**.

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

Securing Trust Protection Platform's web servers

To secure and protect all web services created and used by the system, Trust Protection Platform automatically redirects HTTP requests to HTTPS and provides a server certificate. This method ensures that all inbound authentication processes are secure.

During installation, Trust Protection Platform creates a self-signed Venafi Operational Certificate (VOC) for each Venafi server, and places them in the Venafi Operational Certificate folder of the policy tree.

CAUTION You should never use a self-signed certificate in production. The self-signed certificate generated by the Trust Protection Platform server is for convenience in development or test environments only. For production environments, install your own CA-issued certificate. To replace the self-signed certificate, see [Replacing the \(VOC\) with your own CA-signed certificate](#) in the *Administration Guide*.

Exceptions to HTTPS Redirects

Because encryption is built into the SCEP protocol used by Network Device Enrollment, SSL/TLS is not enforced like it is for other Venafi web services. This is useful for servicing certificate enrollment requests from legacy SCEP clients that do not support SSL/TLS (HTTPS).

Backing up the software encryption key

When you installed and configured Venafi Trust Protection Platform, you had the option to enable either software or hardware encryption (or both). If you enabled software encryption, you need to back up the software encryption key to a secure location. The software key is critical to the functionality of Trust Protection Platform. Without it, you cannot access data in the database. In the event of a system failure, you will need a copy of the encryption key to access your data. Additionally, if you want to install additional Trust Protection Platform servers, you will need the software key to install and configure those servers.

DID YOU KNOW? How is the Venafi Trust Protection Platform software key used and why is it so important to back it up?

Trust Protection Platform maintains all system information—that is, configuration settings, managed server and certificate information, archived certificates, and private keys—in a database. To secure this information, Trust Protection Platform uses an AES-256 encryption key—the software key—to encrypt the connection to the database.

Depending on the encryption key selected in the object configuration, the objects themselves can be encrypted using the software key. The key is securely stored in the Windows registry.

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

To export the software key from Venafi Configuration Console

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

For more information, see [Venafi Configuration Console](#) in the Administration Guide.

To export the software key from the command line

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

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

Adding another server to the Trust Protection Platform network

There are several reasons for adding another server to your Trust Protection Platform network.

Here are a few scenarios:

- You need an application delivery controller or fail-safe server
- You have isolated network segments and a single Trust Protection Platform server can't access your entire network
- You need scalability and have specialized servers dedicated to UI access, performing discoveries, or servicing the agents.

To add another server

1. Copy the Trust Protection Platform installation file (VenafiTPPInstall-25.1.x.msi) to the new server.

Export and copy the software encryption key from the existing server (if the software encryption key is used in your environment).

To learn more, see [Managing the default software encryption key](#).

2. Run the .msi file.

The installation wizard will walk you through the installation process.

Be sure to use the same encryption key(s) from the existing server on the new server so that the database is using the same key(s) on both servers.

3. Follow the onscreen prompts to install Trust Protection Platform on the additional server.

About application delivery controllers

When you have multiple Venafi Trust Protection Platform servers in a cluster, the servers automatically work together to ensure proper load balancing between the Venafi servers in the cluster.

When scheduling daily tasks, the recommended configuration is to schedule them to start at the same time across the servers.

Configuring general SMTP options for outbound email notifications using Policy Tree

After Trust Protection Platform is installed and running, you must configure your simple mail transport protocol (SMTP) settings. By default, SMTP settings are blank. However, these settings are required for sending important notifications about your encryption assets.

TIP You can also complete these tasks in Venafi Configuration Console (VCC) by editing the properties of the Log Channels connector on the Connectors node. For details, see [Setting up SMTP settings for email notifications](#).

To configure notifications

1. From the [Platform menu bar](#), click Policy Tree and go to the **Logging** tree.
2. Click the **Channels** object.
3. On the **Channel Settings** tab, refer to the following table while completing SMTP settings:

[Settings > Channel Settings tab](#)

SMTP Options

Field	Description
Host	Hostname or IP address of the SMTP server. Trust Protection Platform Channel drivers support both IPv4 and IPv6 connections. If a hostname is specified, only the first resolved address associated with that name is used. You can append the port number to the host. For example: <i><hostname>:25</i> .
Credential	Username credential required to authenticate with the SMTP server. Configure this option only if SMTP authentication is configured on your SMTP server. Otherwise, all notifications routed through this Channel object will fail.

Field	Description
Sender	Name that appears in the From: line for all messages sent from this SMTP Channel object. Some SMTP servers require this field to be a valid email address. If this is required by your SMTP server, make sure you provide a valid email address, such as <code>username@yourcompany.com</code>.
Use TLS	Configures the SMTP channel driver to use Transport Layer Security (TLS) to send SMTP notifications. Select this option only if your SMTP server is configured to support TLS. Otherwise, all notifications routed through this Channel object will fail.
Log Delivery	The setting to manage SMTP events regarding delivery success or failure. <i>No:</i> Discard log events. <i>Yes:</i> Log email notifications. For example, the driver fails to connect to the SMTP server. If available, additional information appears in the exception details from the SMTP server. This information is helpful in troubleshooting connectivity and configuration issues.

3

Upgrading Venafi Platform 25.1.x

You can upgrade to Venafi Trust Protection Platform™ 25.1 from any currently supported version (or any supported patched version). To learn more, see ["Trust Protection Platform upgrade options" on page 124](#).

This section outlines the preparatory configurations required to upgrade from an earlier version of Venafi Trust Protection Platform™.

To upgrade to the latest 25.1 release

1. Prepare for your upgrade. Most of these steps should be done before the maintenance window begins.

For specific steps, see ["Preparing to upgrade to 25.1" below](#).

2. During the maintenance window, upgrade each of your Venafi servers.

For specific steps on upgrading using the GUI, see ["Upgrade steps" on page 126](#).

For specific steps on upgrading using the CLI, see ["Upgrade using the command line" on page 138](#).

Preparing to upgrade to 25.1

For detailed upgrade steps, see ["Upgrade steps" on page 126](#).

IMPORTANT If you are using (or plan to use) the Server Agent with Trust Protection Platform, carefully review the [Trust Protection Platform and Server Agent version compatibility table](#) **before** upgrading.

- Decide if you are going to do a rolling upgrade, and if so, which model. See ["About rolling upgrades" on the facing page](#).
- ["Review the release documentation" on page 123](#) for important information related to this upgrade.
- Make sure your origin version is on the latest patch (upgrade may be required).

Venafi strongly recommends that you update to the latest patch of your source version before you upgrade to 25.1.

The Venafi Updater utility enables you to apply maintenance updates to your current version of Venafi Trust Protection Platform™. It does not support product upgrades to newer product releases.

For more information, see ["Updating the latest patch" on page 141](#).

- Review and update your internally-documented upgrade playbook.

Many customers have an internal "playbook" developed with Venafi Professional Services with instructions and policies you need to follow for upgrading your Venafi servers. See if there are new options available or new requirements that need to be documented in your playbook. Review this entire chapter, and compare with your playbook to see where updates may be necessary.

- Schedule a maintenance window.

Most customers use a change management process that requires a scheduled maintenance window for making changes to the production environment. Your change management process may include creating a change request with documents potential risks, as well as risk-mitigation steps you will take to ensure all affected people are aware of the change.

Usually these change requests require an approval process, so give yourself plenty of lead time if these requirements apply to you.

- Download Trust Protection Platform version 25.1. For specific steps see ["Downloading the latest version of Venafi Trust Protection Platform" on page 88](#).
- If you are using an answer file, **you may need to update it before upgrading**. For details on the current answer file schema, see ["Creating and using answer files" on page 89](#).

We recommend you create a new answer file using version 25.1 for use in scripted installations and upgrades.

- Upgrade and test in non-production environments.

Especially when you plan to change features, or if current feature deprecations affect your environment, we highly recommend that you test the upgraded version of Trust Protection Platform against a *recent copy* of your production database to identify any issues before you go live.

WARNING! Never use your production database in lower environments (dev, test, sandbox, etc.)! Always use a recent copy of your production database in lower environments.

IMPORTANT If you have a PS VSE, you must check with your Professional Services Engagement Manager to ensure your VSE is compatible with 25.1. Depending on the features of your VSE and changes implemented between your origin version and 25.1 (the target version), a newer version of the VSE might need to be provided to you by Venafi Professional Services.

About rolling upgrades

When installing or upgrading Venafi Platform, you have several options including options for high-availability (rolling upgrades), and a least-permissions model for database access. These options allow you to:

- Improve high availability by allowing rolling upgrades of servers without needing to take all servers offline simultaneously, which can allow the services the cluster provides to stay online the entire time with the help of application delivery controllers.

You may be concerned about the length of time involved in a rolling upgrade, and if that makes the product "half-updated." In fact, this process was designed so you can leave some servers unpatched for an extended period of time (even weeks) if needed. Of course, while it's preferable to upgrade the entire cluster as quickly as reasonably possible, the system remains fully functioning throughout the entire rolling upgrade process.

- Leverage a least-permissions model for database access, so there is a transactional database user for daily interactions with the database, as well as an account with higher privileges used for installing and upgrading the system.
- Improve the installation and upgrade experience by not requiring database scripts to be run manually, as Trust Protection Platform's upgrade installer uses the higher privileged database account to execute the queries automatically during the upgrade.

This enables enterprise services that depend on Venafi products as part of their pipeline to remain online during Venafi product upgrades. For example, if you have a customer-facing website that spins up web server nodes dynamically according to traffic demands, you may be injecting TLS certificates that are generated on demand from Venafi TLS Protect as part of the build pipeline. This process can continue to function during a Venafi server cluster upgrade because one or more servers remain online throughout the upgrade process.

Supported upgrade models

There are three supported models for upgrading to 25.1.

- **In place rolling upgrade.** When using this upgrade model, you will remove one server at a time from the application delivery controller, upgrade it, and then replace it in the application delivery controller before upgrading the next server. This model requires both redundancy (i.e. all services the cluster provides are provided by at least two servers) and an application delivery controller (so the network traffic can be directed to the online servers while the offline server is being upgraded). This upgrade model results in no outage. This process takes significantly longer than offline upgrades. It also requires multiple configuration changes to the application delivery controller settings throughout the upgrade process. During the upgrade, you need to wait until there are no active connections on the ports that Venafi services before you can perform the upgrade on that Venafi server. For information on the steps for this upgrade model, see ["In place rolling upgrade" on page 127](#).
- **Replace rolling upgrade.** With this upgrade model, you will deploy new Windows servers. After Trust Protection Platform is installed and running on those servers, you will join them to the application delivery controller for the cluster. Finally, you will decommission the servers with the older version of Trust Protection Platform. This model requires you to deploy one new server for each existing server. For example, if you have six Venafi servers on your origin version (that you are upgrading from), you would need to deploy six new Windows servers for the target version, each one matching exactly the configuration of the server it will replace (including Venafi components, processing engine assignments, and network discovery zones).

This model can often result in a cleaner upgrade process, and allows you to upgrade your Windows operating system at the same time you are upgrading your Venafi version, but results in extra manual configuration or steps that need to be scripted. For more information on the steps for this upgrade model, see ["Replace rolling upgrades" on page 130](#).

- **Offline upgrade.** (Not a rolling upgrade) In this model, you take down the entire Venafi server cluster at the same time. You turn off all services on all servers simultaneously. This causes an outage of Venafi service, but allows the upgrade to happen much faster. This model is often suitable for environments that have lower uptime requirements. This model is the only upgrade model that was supported in 19.4 and earlier. For more information on the steps for this upgrade model, see ["Offline upgrade" on page 134](#).

Review each model, and determine which model you will use for your upgrade, as this decision impacts how you will proceed with the upgrade.

What's required

While there are many benefits of rolling upgrades, they take more time, configuration and infrastructure than an offline upgrade. To use a rolling upgrade model, you will need to meet the following requirements:

- **Server role redundancy.** While this is already identified in the system requirements, it is important to evaluate if your cluster meets this requirements. Look at the servers you have in the cluster, what roles they have, and what network segments each server is servicing.

For example, if you have four isolated network segments, and in each segment you have a single Venafi server that is used for discovery, validation, and certificate installation for the TLS Protect product, services in those network segments would be unavailable during an upgrade unless additional Venafi servers were brought online to cover those segments. For this example, you might consider the Replace Rolling Upgrade model, as the redundancy is only required during the upgrade process.

If redundancy for fault tolerance is important to your organization's overall high availability requirements, you should consider deploying additional servers to each isolated network segment permanently.

- **Application delivery controller.** All Venafi web services should be made available to clients through an application delivery controller (load balancer). This requirement allows one or more servers in the resource pool to be offline while still providing access through the same web service endpoint.

Typically in either rolling upgrade model changes to the application delivery controller configuration are required during the upgrade to ensure new client connections are not routed to a server that is involved in an upgrade.

Review the release documentation

Venafi believes that keeping up with the most recent versions of the platform is in the best interest of all customers. To ensure a successful upgrade, we've documented the information below for you to review and consider as you plan your production upgrade.

- [Important Upgrade Considerations.](#)

IMPORTANT Read the entire list of Important Upgrade Considerations before upgrading your production environment to version 25.1.

- [What's new in 25.1.](#)
- For resolved issues, known issues visit the [Readme](#).
- [Deprecated Functionality From Venafi Platform.](#)
- [Functionality Scheduled For Deprecation.](#)

Trust Protection Platform upgrade options

Trust Protection Platform supports several upgrade options, allowing for high availability but slower upgrades, or faster upgrades with service interruption. Please consider the following items as you upgrade:

- Venafi provides product support for two years (24 months) of Trust Protection Platform versions. Venafi also provides upgrade support from any supported version to the current version.
- You must be on a supported origin version (or any supported patch) before you upgrade to 25.1.
- You do not need to uninstall Trust Protection Platform prior to upgrading. You can install new versions over older versions.
- You can download the currently-supported versions of Trust Protection Platform by signing into your Venafi account at download.venafi.com.
- There are three different upgrade strategies. See "About rolling upgrades" on page 121 to help you select the correct strategy for your organization.
 - Offline upgrade
 - In-place rolling upgrade
 - Replace rolling upgrade
- Be sure to check out the Important Upgrade Considerations section in your version-specific documentation for the intermediate version before upgrading.

Upgrading from an unsupported version of Trust Protection Platform

If you are running an unsupported version of Trust Protection Platform (which is any version including 22.3 or older), you cannot directly upgrade to the current version. You must follow a recommended upgrade path that involves two steps:

1. First, upgrade to at least the minimum supported version. For example, if your origin version is 22.2.x, you need to upgrade to at least version 23.1.x (the minimum supported version).
2. Once your entire cluster has been upgraded to the supported version 23.1.x, you can then migrate the entire cluster to the current version 25.1.x.

In summary, the upgrade path would be: 22.2 -> 23.1 -> 25.1.

The following table lists the patch versions that have been tested for compatibility with the 25.1 release.

Origin version

22.4.x

23.1.x

23.3.x

24.1.x

24.3.x

TIP You may have noticed that the instructions said you needed to be on the oldest supported version, 23.1, but the upgrade table says you can upgrade from version 22.4.

If you are currently on version 22.4 you *can* directly upgrade to version 25.1, as version 22.4 was supported until 25.1 was released.

However, if you are starting from a version older than 22.4, you will want to upgrade to 23.1 (or later) so if you encounter any issues during the upgrade, you can get assistance from Venafi Customer Support.

Server Agent upgrade options

Server Agent 25.1 supports upgrades with the full installation package on all OS platforms. Before you upgrade, please consider the following:

- Agent Upgrade Work is bit-specific. Agent Upgrade Work cannot update a 32-bit Server Agent to the 64-bit version. You must use the full installer to upgrade from 32-bit to 64-bit.
- Agent Upgrade Work will not send versions that are not listed in the table below. In cases where the work isn't sent, then multi-stage upgrades via an intermediate version may be available. Performing an upgrade via full platform-specific installer is always an option.

Server Agent 25.1 supported upgrade paths for Venafi Update package:

Current version	Operating system	Final version
22.2.x, 22.3.x, 22.4.x	All, including Linux, Solarix, AIX	25.1
23.1.x, 23.3.x	All, including Linux, Solarix, AIX	25.1

Upgrade steps

Use the information in this section when you are performing the upgrades on the servers in your cluster. This section includes specific upgrade steps for the three supported upgrade models. These upgrade models are:

- **In place rolling upgrade.** When using this upgrade model, you will remove one server at a time from the application delivery controller, upgrade it, and then replace it in the application delivery controller before upgrading the next server. This model requires both redundancy (i.e. all services the cluster provides are provided by at least two servers) and an application delivery controller (so the network traffic can be directed to the online servers while the offline server is being upgraded). This upgrade model results in no outage. This process takes significantly longer than offline upgrades. It also requires multiple configuration changes to the application delivery controller settings throughout the upgrade process. During the upgrade, you need to wait until there are no active connections on the ports that Venafi services before you can perform the upgrade on that Venafi server. For information on the steps for this upgrade model, see ["In place rolling upgrade" on the facing page](#).
- **Replace rolling upgrade.** With this upgrade model, you will deploy new Windows servers. After Trust Protection Platform is installed and running on those servers, you will join them to the application delivery controller for the cluster. Finally, you will decommission the servers with the older version of Trust Protection Platform. This model requires you to deploy one new server for each existing server. For example, if you have six Venafi servers on your origin version (that you are upgrading from), you would need to deploy six new Windows servers for the target version, each one matching exactly the configuration of the server it will replace (including Venafi components, processing engine assignments, and network discovery zones).

This model can often result in a cleaner upgrade process, and allows you to upgrade your Windows operating system at the same time you are upgrading your Venafi version, but results in extra manual configuration or steps that need to be scripted. For more information on the steps for this upgrade model, see ["Replace rolling upgrades" on page 130](#).

- **Offline upgrade.** (Not a rolling upgrade) In this model, you take down the entire Venafi server cluster at the same time. You turn off all services on all servers simultaneously. This causes an outage of Venafi service, but allows the upgrade to happen much faster. This model is often suitable for environments that have lower uptime requirements. This model is the only upgrade model that was supported in 19.4 and earlier. For more information on the steps for this upgrade model, see ["Offline upgrade" on page 134](#).

In place rolling upgrade

Use the in place rolling upgrade model when all existing Venafi servers will be updated to 25.1, but because you have redundancy and an application delivery controller, and because you are only doing servers one server at a time all services that the cluster provides can remain available throughout the upgrade. This upgrade results in no outage. This process takes significantly longer than offline upgrades. It also requires multiple configuration changes to the application delivery controller settings throughout the upgrade process. During the upgrade, you need to wait until there are no active connections on the ports that Venafi services before you can perform the upgrade on each Venafi server.

When performing this upgrade, follow all the steps in each of the following sections.

Getting Started

1. Download, distribute, and unzip installation files for the 25.1.x upgrade.
2. [Optional] Export your software encryption key (if used).

For more information, see ["Backing up the software encryption key" on page 114](#).

3. Update your application delivery controller to remove the first Venafi server from the resource group.
4. Wait until there are no active connections.

NOTE Use a utility like `netstat -an | findstr ESTABLISHED` to verify that there are no established (active) connections on the IIS listening IP/Ports. Do not continue until there are no active connections (or these users will experience down time).

Begin the upgrade

1. On the Venafi server being upgraded, open Venafi Configuration Console and click the **Product** node.
2. Stop all Venafi services running on the Windows Server, including:
 - Venafi Platform
 - Venafi Log Server (Logging)
 - API Host
 - Website (IIS)

- JavaKeyHost Service
- Enrollment over Secure Transport Service

NOTE When you stop Venafi Windows services, be aware that the services may have been manually configured to recover on failures by automatically restarting services. In this case you will either want to reset your recovery options to "Take no Action" or disable the service altogether before proceeding.

If services are set to automatically restart, the upgrade can fail.

3. Close the Venafi Configuration Console and all other Venafi-related applications (VCC, Venafi Support Tool, etc.).

If multiple user accounts connect to the Venafi server, use the Task Manager Users tab to terminate any background user sessions from other logged-in users. This ensures that no Venafi files are in use by any user, making the upgrade process more efficient.

Database configuration

1. Back up your database.

For instructions on how to perform the database backup, visit Microsoft's SQL documentation: [Create a Full Database Backup](#).

2. *[Conditional] If using answer file(s):* Update the answer file so the DBO credentials are included, and new components (if desired) are added to the appropriate servers.

For detailed information about the schema and settings of the answer file, see "Creating and using answer files" on page 89.

Run the installation MSI

1. Verify that the extracted `Venafi Trust Protection Platform 25.1.x.zip` is available on the server.
2. From an elevated command prompt, change your directory to the extracted zip folder and enter the following command:

```
VenafiTPPInstall-25.1.x.msi
```

How to open an elevated command prompt

- a. From the Start menu, search for `CMD`.
- b. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Why do I need an elevated command prompt?

Running VenafiTPPInstall-25.1.x.msi from an elevated command prompt ensures that:

- The Venafi Configuration Console launches properly after the installation is complete.
 - You can uninstall Trust Protection Platform from Windows' **Programs and Features** tool without needing to run a special command in an elevated command prompt.
3. When the Welcome window appears, click **Next**.
 4. Read the terms stated in the License Agreement window. If you agree, select **I accept the terms in the license agreement**, and then click **Next**.

Configure the server

1. Either use the configuration wizard GUI to complete the configuration steps for the upgrade, or use the `TPPConfiguration.exe` CLI to do a silent upgrade using the appropriate updated answer file.

If you have questions about the command line interface, see ["Upgrade using the command line"](#) on page 138.

For information about the TPPConfiguration utility, see ["Using the TppConfiguration command line tool"](#) on page 99.

To configure Venafi Trust Protection Platform using the Venafi Configuration Console

- a. On the **Welcome** screen, review the information, and then click **Next**.

If you have any questions about fields in this wizard, refer to the field-specific information in ["Configure Venafi platform from the Venafi Configuration Console"](#) on page 69.
- b. On the **Administrative Account** screen, enter the local master admin credentials for Trust Protection Platform, and then click **Next**.
- c. On the **Database Settings screen**, enter the information for the database owner account: **type**, **login**, and **password**.

For information about the Settings tab, see ["Field descriptions - Settings tab"](#) on page 73.

For information about the Expert tab, see ["Field descriptions - Expert tab"](#) on page 76.

- d. On the **Customer Experience** screen, review the information on how data is collected.

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

- e. On the **Upgrade Server** screen, review the information, and then click **Finish**.
- f. When the configuration is complete, click **Close**.

Once you have completed the configuration wizard, the Venafi Configuration Console window automatically opens. For more information about how to use the Venafi Configuration Console, see [Venafi Configuration Console](#).

2. *[Conditional] If you used the upgrade wizard GUI in step 1:* In the Venafi Configuration Console, enable any new components that you want for each server.
3. In the Venafi Configuration Console, click the **Product** node.
4. Start all Venafi Windows services.
5. If this server has the WebConsole component installed, open the console (without the application delivery controller; for example, use `https://localhost/Aperture`)
6. Update your application delivery controller by placing this server back into the resource group.
7. Repeat all steps (starting with the Getting Started section above) for the next Venafi server.

Validate the installation

- Validate that each server in the cluster is performing its assigned role.

For example, on a server that has the Venafi Web Console, try renewing a certificate or rotating an SSH key. On a code signing server, try signing code. For a server, validate that connections are happening as expected.

Replace rolling upgrades

The replace rolling upgrades model involves deploying new Windows servers that you are installing 25.1 on, and joining them to your existing Venafi database for the cluster, then replacing the existing servers with the new servers. It requires you deploy one new server for each existing server. For example, if you

have six Venafi servers on your origin version (that you are upgrading from), you would need to deploy six new Windows servers, each one matching exactly the configuration of the server it will replace (including Venafi components, processing engine assignments, and network discovery zones).

This model can often result in a cleaner upgrade process, and allows you to upgrade your Windows operating system at the same time you are upgrading your Venafi version, but results in extra manual configuration or steps that need to be scripted.

When performing this upgrade, follow all the steps in each of the following sections.

Getting Started

1. Create new Windows servers that match 1:1 the roles of the servers in your current Venafi deployment cluster.
2. Download, distribute, and unzip installation files for the 25.1.x upgrade.
3. [Optional] Export your software encryption key (if used).

For more information, see ["Backing up the software encryption key" on page 114](#).

Database configuration

1. Back up your database.

For instructions on how to perform the database backup, visit Microsoft's SQL documentation: [Create a Full Database Backup](#).

2. *[Conditional] If using answer file(s):* Update the answer file so the DBO credentials are included, and new components (if desired) are added to the appropriate servers.

For detailed information about the schema and settings of the answer file, see ["Creating and using answer files" on page 89](#).

Run the installation MSI

1. Verify that the extracted `Venafi Trust Protection Platform 25.1.x.zip` is available on the server.
2. From an elevated command prompt, change your directory to the extracted zip folder and enter the following command:

VenafiTPPInstall-25.1.x.msi

How to open an elevated command prompt

- a. From the Start menu, search for `CMD`.
- b. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Why do I need an elevated command prompt?

Running VenafiTPPInstall-25.1.x.msi from an elevated command prompt ensures that:

- The Venafi Configuration Console launches properly after the installation is complete.
 - You can uninstall Trust Protection Platform from Windows' **Programs and Features** tool without needing to run a special command in an elevated command prompt.
3. When the Welcome window appears, click **Next**.
 4. Read the terms stated in the License Agreement window. If you agree, select **I accept the terms in the license agreement**, and then click **Next**.
 5. Run the previous steps on all the new Windows Venafi server. Do not modify your existing (production) servers.

Configure the server

1. Either use the configuration wizard GUI to complete the configuration steps for the upgrade, or use the `TPPConfiguration.exe` CLI to do a silent upgrade using the appropriate updated answer file.

If you have questions about the command line interface, see ["Upgrade using the command line" on page 138](#).

For information about the TPPConfiguration utility, see ["Using the TppConfiguration command line tool" on page 99](#).

To configure Venafi Trust Protection Platform using the Venafi Configuration Console

- a. On the **Welcome** screen, review the information, and then click **Next**.

If you have any questions about fields in this wizard, refer to the field-specific information in ["Configure Venafi platform from the Venafi Configuration Console" on page 69](#).

- b. On the **Administrative Account** screen, enter the local master admin credentials for Trust Protection Platform, and then click **Next**.

- c. On the **Database Settings** screen, enter the information for the database owner account: **type**, **login**, and **password**.

For information about the Settings tab, see ["Field descriptions - Settings tab"](#) on page 73.

For information about the Expert tab, see ["Field descriptions - Expert tab"](#) on page 76.

- d. On the **Customer Experience** screen, review the information on how data is collected.

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

- e. On the **Upgrade Server** screen, review the information, and then click **Finish**.

- f. When the configuration is complete, click **Close**.

Once you have completed the configuration wizard, the Venafi Configuration Console window automatically opens. For more information about how to use the Venafi Configuration Console, see [Venafi Configuration Console](#).

2. *[Conditional] If you used the upgrade wizard GUI in step 1:* In the Venafi Configuration Console, enable any new components that you want for each server.
3. In the Venafi Configuration Console, click the **Product** node.
4. Start all Venafi Windows services.
5. If this server has the WebConsole component installed, open the console (without the application delivery controller; for example, use <https://localhost/Aperture>)
6. Repeat on all Venafi servers.

Configure the application delivery controller

1. Update your application delivery controller to add all the new Windows servers to the resource group.
2. Update your application delivery controller to remove the old Windows servers from the resource group.
3. Wait until there are no active connections.

NOTE Use a utility like `netstat -an | findstr ESTABLISHED` to verify that there are no established (active) connections on the IIS listening IP/Ports. Do not continue until there are no active connections (or these users will experience down time).

4. Uninstall Venafi Trust Protection Platform from all old Venafi servers.

For additional information, see ["Uninstalling Venafi Trust Protection Platform" on page 142](#).

5. Remove all old Venafi servers (engines) from the Venafi cluster in Policy Tree.

How do I delete a server from the Venafi cluster in Policy Tree?

- a. Navigate to the Platform product, click **Policy Tree**, then select the **Platforms** tree.
- b. Right-click on the server you want to remove, then click **Delete**.
- c. Confirm the removal (twice).

Validate the installation

- Validate that each server in the cluster is performing its assigned role.

For example, on a server that has the Venafi Web Console, try renewing a certificate or rotating an SSH key. On a code signing server, try signing code. For a server, validate that connections are happening as expected.

Offline upgrade

The offline upgrade model requires turning off all services on all servers simultaneously. This causes an outage of Venafi service, but allows the upgrade to happen faster. In addition, it's often suitable for environments that have lower up-time requirements. This model is familiar to many Venafi system administrators because it was the only upgrade model that was supported in 19.x and below.

When performing this upgrade, follow all the steps in each of the following sections.

Getting Started

1. Download, distribute, and unzip installation files for the 25.1.x upgrade.
2. [Optional] Export your software encryption key (if used).

For more information, see ["Backing up the software encryption key" on page 114](#).

Begin the upgrade

1. On the Venafi server being upgraded, open Venafi Configuration Console and click the **Product** node.
2. Stop all Venafi services running on the Windows Server, including:
 - Venafi Platform
 - Venafi Log Server (Logging)
 - API Host
 - Website (IIS)
 - JavaKeyHost Service
 - Enrollment over Secure Transport Service

NOTE When you stop Venafi Windows services, be aware that the services may have been manually configured to recover on failures by automatically restarting services. In this case you will either want to reset your recovery options to "Take no Action" or disable the service altogether before proceeding.

If services are set to automatically restart, the upgrade can fail.

3. Close the Venafi Configuration Console and all other Venafi-related applications (VCC, Venafi Support Tool, etc.).

If multiple user accounts connect to the Venafi server, use the Task Manager Users tab to terminate any background user sessions from other logged-in users. This ensures that no Venafi files are in use by any user, making the upgrade process more efficient.

4. Repeat these steps on all Venafi servers to ensure the entire cluster is shut down before continuing.

Database configuration

1. Back up your database.

For instructions on how to perform the database backup, visit Microsoft's SQL documentation: [Create a Full Database Backup](#).

2. *[Conditional] If using answer file(s):* Update the answer file so the DBO credentials are included, and new components (if desired) are added to the appropriate servers.

For detailed information about the schema and settings of the answer file, see ["Creating and using answer files" on page 89](#).

Run the installation MSI

1. Verify that the extracted `Venafi Trust Protection Platform 25.1.x.zip` is available on the server.
2. From an elevated command prompt, change your directory to the extracted zip folder and enter the following command:

```
VenafiTPPInstall-25.1.x.msi
```

How to open an elevated command prompt

- a. From the Start menu, search for `CMD`.
- b. In the search results, right-click on **Command Prompt**, and choose **Run as administrator**.

Why do I need an elevated command prompt?

Running `VenafiTPPInstall-25.1.x.msi` from an elevated command prompt ensures that:

- The Venafi Configuration Console launches properly after the installation is complete.
 - You can uninstall Trust Protection Platform from Windows' **Programs and Features** tool without needing to run a special command in an elevated command prompt.
3. When the Welcome window appears, click **Next**.
 4. Read the terms stated in the License Agreement window. If you agree, select **I accept the terms in the license agreement**, and then click **Next**.
 5. Run the previous step on all Venafi servers. This can be done one at a time, or can be done simultaneously.

Configure the server

1. Either use the configuration wizard GUI to complete the configuration steps for the upgrade, or use the `TPPConfiguration.exe` CLI to do a silent upgrade using the appropriate updated answer file.

If you have questions about the command line interface, see ["Upgrade using the command line" on page 138](#).

For information about the TPPConfiguration utility, see ["Using the TppConfiguration command line tool"](#) on page 99.

To configure Venafi Trust Protection Platform using the Venafi Configuration Console

- a. On the **Welcome** screen, review the information, and then click **Next**.

If you have any questions about fields in this wizard, refer to the field-specific information in ["Configure Venafi platform from the Venafi Configuration Console"](#) on page 69.

- b. On the **Administrative Account** screen, enter the local master admin credentials for Trust Protection Platform, and then click **Next**.
- c. On the **Database Settings** screen, enter the information for the database owner account: **type**, **login**, and **password**.

For information about the Settings tab, see ["Field descriptions - Settings tab"](#) on page 73.

For information about the Expert tab, see ["Field descriptions - Expert tab"](#) on page 76.

- d. On the **Customer Experience** screen, review the information on how data is collected.

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

- e. On the **Upgrade Server** screen, review the information, and then click **Finish**.
- f. When the configuration is complete, click **Close**.

Once you have completed the configuration wizard, the Venafi Configuration Console window automatically opens. For more information about how to use the Venafi Configuration Console, see [Venafi Configuration Console](#).

2. *[Conditional]* If you used the upgrade wizard GUI in step 1: In the Venafi Configuration Console, enable any new components that you want for each server.
3. In the Venafi Configuration Console, click the **Product** node.
4. Start all Venafi Windows services.
5. Repeat on all Venafi servers.

Validate the installation

- Validate that each server in the cluster is performing its assigned role.

For example, on a server that has the Venafi Web Console, try renewing a certificate or rotating an SSH key. On a code signing server, try signing code. For a server, validate that connections are happening as expected.

Upgrade using the command line

When you run the command line utility, the system checks to see if this is a new installation on the Venafi Trust Protection Platform server, or if this is an upgrade of existing software.

The process to upgrade the existing software using the command line is the same as for installing using the command line. Please refer to the command line installation instructions for details on how to script the installation and configuration of Trust Protection Platform. See "[Command line installation and configuration](#)" on page 87.

NOTE You need to have installed the MSI on the Venafi Trust Protection Platform server either as a manual step, or using a script.

To upgrade using the command line utility

1. On each Venafi Trust Protection Platform server download version 25.1.x of Trust Protection Platform, and extract the zip file.
2. Open an elevated command prompt, and run the MSI file using the following command:

```
msiexec /i "[Staging_Directory]\Product\VenafiTPPInstall-25.1.x.msi" /q /n
```

The `x` in the previous command represents the "dot version." For the major release, the "dot version" is 0. For patches, it is a number greater than 0.

You *do not* need to install a major release before you can install a patch; we recommend installing the latest patched version of Venafi Platform.

For example, if you are installing version 25.1.1, use the following command:

```
msiexec /i "[Staging_Directory]\Product\VenafiTPPInstall- 25.1.1.msi" /q /n
```

3. From the command prompt browse to the `Venafi\Platform` directory.

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

```
C:\Program Files\Venafi\Platform
```

4. Run the configuration utility (`TppConfiguration.exe`) with the `-install` switch.

```
TppConfiguration.exe -install:C:\answerfile.xml -password:[encrypted answer file password]
```

For details about how to use the TppConfiguration utility, see ["Using the TppConfiguration command line tool"](#) on page 99.

Upgrade status icon and page

Your upgrade to 25.1 consists of two processes:

- Each engine connected to the database gets upgraded to 25.1.
- The database gets upgraded to the 25.1 schema.

If you are using an offline upgrade, both of these processes are typically complete before you restart the Venafi services on the engines, so the upgrade is completed while all engines are off-line. For details, see ["Offline upgrade"](#) on page 134.

If you are using one of the rolling upgrade methods, there will be a time of version inconsistency as the upgrade rolls out; some servers that have yet to be updated will be on the previous version while others will have been successfully upgraded to 25.1. This also applies to stored data in the database as the system upgrades to the format used in 25.1. For information on our rolling upgrade options, see ["Upgrade steps"](#) on page 126

When an upgrade is in progress, an "upgrade in progress" icon is displayed on the right side of the menu bar. This animated icon alerts all users that because an upgrade is in progress, system performance may be impacted.

Users with access to the Platform product can click the icon to see the upgrade status for each engine and the databases in the cluster, and will see a modified icon if there is an error during upgrade. You can either click the upgrade status icon and will be automatically redirected, or you can manually navigate to your **user account** icon > **About** > **Upgrade Status**.

The upgrade status page shows you all the engines and their current status. A blocked icon is shown next to servers that are waiting for something before the upgrade can continue. Click the expand arrow next to the engine name to see the upgrade tasks and statuses for a specific engine.

The upgrade status icon and status page not only notify you about the status of your rolling upgrades, but more importantly, it enables you to better manage those upgrades by helping you quickly identify and resolve potential issues without needing to contact Support.

The same information available on this page is available using the WebSDK using a series of `SystemStatus/Upgrade` endpoints, such as [GET SystemStatus/Upgrade/Summary](#) in the Venafi Developer's Guide.

4

Updating the latest patch

Updates to a major release of Trust Protection Platform are called *patches*. Any patches released for 25.1 will have a version of 25.1.x, where x is a number greater than 0.

As of 20.4, upgrading to a patched version is the same all other upgrades:

- Download the patch.

The patch is an .msi file. On the download page, you will see the major release, and the latest patch. Since patches are cumulative, you only need the most recent one.

For more information, see ["Downloading the latest version of Venafi Trust Protection Platform" on page 88](#)

- Upgrade using ["Upgrading Venafi Platform 25.1.x " on page 119](#).

You can use any of the supported upgrade methods including:

- ["In place rolling upgrade" on page 127](#)
- ["Replace rolling upgrades" on page 130](#)
- ["Offline upgrade" on page 134](#)

- You can also upgrade using the command line. For details, see ["Upgrade using the command line" on page 138](#).

5

Uninstalling Venafi Trust Protection Platform

You can uninstall Trust Protection Platform from either the command line or by using the Windows Control Panel.

The uninstall process removes program files, services, shortcuts, and registry keys.

The files that are maintained when you uninstall are:

- \Program Files\Venafi\Logs\TPP Configuration Log.txt
- \Program Files\Venafi\Logs\TPP Configuration Log.txt.reg

The .reg file is a backup of everything that we removed from the registry by the un-installation process.

NOTE There are items in this file that are not portable. That means you cannot import this file on a new Windows server and expect to use it to restore on the new machine. Instead, re-install on the new machine using the software or hardware key used to encrypt this system.

Using the command line

1. Log in as a user with Administrator privileges.
2. Right-click the Command Line program icon, and select **Run as Administrator**.
3. Run the following command:

```
msiexec /uninstall path_to_director_msi
```

Using the Windows Control Panel

TIP If you did not run the MSI installer using elevated privileges, you might not be able to use this method to uninstall Trust Protection Platform.

1. Go to the **Windows Control Panel**.
2. Click **Start > Control Panel > Programs > Programs and Features**.
3. Select **Venafi Trust Protection Platform (64-bit)**, and then click **Uninstall**.
4. When the uninstall process finishes, click **Finish**.

6

Disaster recovery operations

This section describes how to recover from a Trust Protection Platform server loss and how to set up standby Trust Protection Platform servers. When a server loss does occur, it is typically due to one of the following reasons:

- The database has been corrupted or deleted.
- The HSM connection has failed or the PIN has changed
- The Trust Protection Platform server itself has encountered a serious error.

This chapter contains the following topics:

High availability disaster recovery	145
Before you begin disaster recovery procedures	146
How to recover a lost Trust Protection Platform server	146
How to recover a lost Trust Protection Platform database (Microsoft SQL)	147
How to recover a broken HSM connection	147

High availability disaster recovery

Venafi Trust Protection Platform supports a High Availability architecture that supports both fault tolerance and disaster scenarios.

Fault tolerance

Fault Tolerant clusters are achieved by having redundancy across all required Venafi services so that if any particular Trust Protection Platform server goes down, there are other Trust Protection Platform servers ready to do the same work. This is why the minimum number of recommended Trust Protection Platform servers is two, even for small deployments.

In order to achieve fault tolerance on the database layer, we recommend configuring AlwaysOn high-availability groups on your Microsoft SQL Server so that standby nodes are able to resume the work if the active node of the database goes down. See ["AlwaysOn high-availability disaster recovery solution"](#) on page 63.

High availability disaster recovery

In order to plan for scenarios where an entire data center may go offline, you may need to replicate your infrastructure to a secondary data center designated for disaster recovery. The Trust Protection Platform servers in this data center may need to be configured in standby mode so that they don't attempt work over a high-latency connection to the active database node, and only activate during a disaster scenario where services are transferred to the disaster recovery data center.

Trust Protection Platform standby mode

Trust Protection Platform supports configuring each server in standby mode. When in standby mode, the Trust Protection Platform server continues run normally, except that no scheduled work is picked up. Trust Protection Platform servers in automatic standby mode will monitor the database connection for latency, and if the latency drops below a configured threshold, which would occur during a disaster scenario, then the Trust Protection Platform server will automatically activate and pick up work.

Standby Mode is an advanced cluster configuration that Venafi Professional Services can help you configure. It isn't currently available for customers to configure independently.

When Standby mode is configured on any server, the [System Status Dashboard](#) will indicate if the Standby servers are idling or active. The dashboard will also indicate the reason a Standby server went active.

In addition to monitoring database latency, Standby mode can be configured to activate based on the work queue size. If the primary Trust Protection Platform engines cannot keep up with the current work demands, the standby Trust Protection Platform servers can come out of idle and start picking up work until the work queue drops below the configured threshold. This configuration is best used for auto scaling use cases instead of automatic disaster recovery use cases, as it will only be useful if the latency to the database is low.

Before you begin disaster recovery procedures

Before following recovery procedures, review the following prerequisites:

- You must know your Trust Protection Platform local master administrator account credentials.
If you do not know your master administrator credentials, you must contact Venafi ["Support Services"](#) on page 150.
- (Conditional) To recover a lost Trust Protection Platform database, you must have a backup copy.
You will also need to know your database connection information.
- (Conditional) To recover a lost Trust Protection Platform server, you'll need a backup copy of your software key or hardware key.

How to recover a lost Trust Protection Platform server

If your Trust Protection Platform server crashes and you cannot revive it, you might need to recover using the following method.

To recover from a Trust Protection Platform server loss

1. On the new server where you plan to install Trust Protection Platform, run the install MSI, and then follow the instructions in the Venafi Configuration Console.
2. If you use software encryption, locate the software encryption key used to protect the Trust Protection Platform database so you can access your system data.

See ["Backing up the software encryption key"](#) on page 114 in the *Venafi Trust Protection Platform Installation Guide*.

3. If you use hardware encryption, you will need to know your HSM connection information.

This is required when you configure Trust Protection Platform.

4. During installation, connect to your database.

For Trust Protection Platform installation details, see ["Installing using the Venafi Configuration Console wizard" on page 67](#) in the *Venafi Trust Protection Platform Installation Guide*.

How to recover a lost Trust Protection Platform database (Microsoft SQL)

If you have lost your Trust Protection Platform database and cannot recover it, you'll need to use a backup copy of your database to restore Trust Protection Platform functionality.

To recover from a lost Trust Protection Platform database

1. Shut down all Venafi services on all servers.
2. Recover your database from a file or a preferred application.
3. Recover users.
4. To ensure that logging and notifications continue to work, restart the service broker for the database.

To verify if the service broker is enabled, run the following query:

```
SELECT is_broker_enabled FROM sys.databases WHERE name = 'Database_name';
```

If it is enabled, you should see a 1 under the "is_broker_enabled" column.

If it is set to "0," then stop all Venafi services again and run the following command:

```
ALTER DATABASE Database_name SET ENABLE_BROKER
```

5. Reconnect the application.

How to recover a broken HSM connection

If your connection between Trust Protection Platform and your HSM is broken or corrupted, you will need to use the following steps to reconnect, or reconfigure the connection between the two.

You can do this either in the Venafi Configuration Console or using the command line.

To reconfigure the connection between Trust Protection Platform and an HSM using Venafi Configuration Console

1. On the Venafi server, open the Venafi Configuration Console.

When the console loads, it will display an error message, saying the connection to the HSM failed to initialize.

IMPORTANT When the console opens, only use the console to reconnect the HSM. Do not attempt to use the console to perform other functions until the connection to the HSM has been restored.

2. Complete the steps to create an HSM connector. For more information, see [Creating a HSM \(Cryptoki\) connector](#) in the Administration Guide.

To reconfigure the connection between Trust Protection Platform and an HSM using the command line

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

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

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

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

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

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

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

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

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

For more information on using the command line to perform actions in Trust Protection Platform, see ["Configure the platform using a script through the command line" on page 97 in the Installation and Upgrade Guide.](#)

A

Appendix A: Contact information

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/>

Support Services

Venafi Customer Support

Phone: 877-266-5159

Email: support@venafi.com

URL: <https://community.cyberark.com>

#

64-bit 48

A

ACME 80

certbot 80

agent api 83

AlwaysOn Availability Groups 63, 67

Amazon Web Services versions

supported 34

Apache HTTP Server

supported versions 34

automatic credential rotation 110

Automatic Layout Manager 80

Azure

supported versions 36

B

Big-IP LTM

supported versions 35

Bulk Provisioning 81

C

CA import 81

CAPI

supported versions 36

CDP 82

certificate lifecycle 81

Citrix NetScaler

supported versions 34

CLI command attributes 110

Client API 83

Code Signing Client Distribution 83

Code Signing Key Server 83

command line configuration 99

command-line interface 99, 110

compatibility

hardware integrations with Venafi 37

software integrations with Venafi 37

configuration console 147

credential rotation 110

credentials 110

CRL 82

CRL Distribution Point 82

CyberArk Enterprise Password Vault

supported versions 34

D

database

AlwaysOn Availability Groups (failover) 67

encrypting 67

Microsoft SQL Server 60

Microsoft SQL Server Enterprise Edition 59

Microsoft SQL Server Standard Edition 59

preparation for creating 59

Dell iDRAC

supported versions 34

deprecated features 119

disaster recovery 144

standby mode 145

DPAPI key

back up or restore 114

drivers

64-bit 48

F

failover 63

fault tolerance 145

fix HSM pin 147

G

gMSA 65

group managed service accounts 65

H

hardware requirements

Trust Protection Platform 7

high availability 145

HP iLO

supported versions 35

HSM 48, 147

HSM Backend 84

HSM pin rotation 110

I

IBM ConnectDirect

supported versions 35

IBM DataPower

supported versions 35

IBM Global Security Kit

supported versions 35

IBM GSK

supported versions 35

IBM TeaLeaf Passive Capture Application

supported versions 35

IBM Tealeaf PCA

supported versions 35

Imperva MX

supported versions 35

install patch 141

installation

ACME Service component 80

Aperture component 80

Automatic Layout Manager component 80

Bulk Provisioning component 80

CA Import component 80

Certificate Lifecycle and Monitoring
component 80

Client REST component 80

components available 80

database configuration 67

- HSM Backend 80
- Network Device Enrollment component 80
- Network Discovery component 80
- Object Monitoring component 80
- Onboard Discovery Manager component 80
- Reporting component 80
- SSH Key Detection and Remediation component 80
- things to do afterwards 113
- Trust Protection Platform 67
- User Pre-enrollment component 80
- Validation component 80
- Web SDK component 80
- WebAdmin component 80
- installation and configuration overview 66
- installation, Server Encryption Manager 66
- installation, Trust Protection Platform
 - overview 39
 - preparation 41
 - upgrading 119

J

JCEKS

supported versions 36

JKS

supported versions 36

L

load balancer 116

load balancing 116

M

Microsoft Azure

supported versions 36

Microsoft SQL Server 60

Microsoft Windows Certificate Store (CAPI)

supported versions 36

Monitoring 85

Mozilla Network Security Services (NSS)

supported versions 36

N

network device enrollment 84

Network Discovery 85

Next Gen Firewall

supported versions 36

notifications 117

configuring 117

NSS

supported versions 36

O

OCSP 82

offline upgrade 134

Onboard Discovery 86

Oracle iPlanet Web Server

supported versions 36

Oracle Java Keystore (JKS and JCEKS)

supported versions 36

P

Palo Alto Networks

supported versions 36

patch

installing 141

patching 141

PEM

supported versions 36

placement jobs 80

post-installation procedures 113

professional services 145

Q

quiet install 87

quiet installation 87

quiet upgrade 87

R

repair HSM 147

reporting 86

resolution

monitor 7

revocation 82

revocation checking 82

enabling 82

revocation monitoring 82

Riverbed SteelHead

supported versions 37

RSA PKCS#12

supported versions 37

S

script install 87

script installation 87

server

adding another 116

Server Agent

supported operating systems 7

Server Encryption Manager

installation 66

uninstalling 142

service accounts 65

services

starting Venafi 113

silent install 87

silent installation 87

silent upgrade 87

sleep 145

SMTP

configure in channel settings for
notifications 117

software key 146

SSH 86

SSH Certificate 86

standby mode 145

starting and stopping Trust Protection
Platform 113

SteelHead WAN Optimizer

supported versions 37

Sun Java System Web Server

see Oracle iPlanet Web Server 36

supported

enrollment and revocation drivers 7

operating systems and hardware

Enterprise Mobility Agent 7

Server Agent 7

Trust Protection Platform server 7

vendors, products, and versions 7

Symantec SSL Visibility Appliance

supported versions 37

system recovery 146

system requirements 7

Trust Protection Platform 7

T

time stamp service 86

time stamping 86

tppconfig 99

tppconfiguration 99

tppconfiguration.exe 99

Trust Protection Platform

HTTPS 114

installing 66

SSL 114

trust anchor for 114

U

unattended install 87

unattended installation 87

uninstalling Server Encryption Manager 142

uninstalling Venafi Trust Protection
Platform 142

Universal C Runtime 7

upgrade 134

upgrading

important considerations before you
upgrade 119

to 25.1 119

V

validation 86

VAM nShield

supported versions 34

Venafi Configuration Console

starting and stopping services 113

Venafi Operational Certificate 114

VOC

see Venafi Operational Certificate 114

W

Web SDK 87

WebSDK 87

Windows authentication

permission requirements 64

Windows Server 2008

Universal C Runtime 7