Cryptographic Security Platform

Vault 10.6.1 installation and administration

Document issue: 1.0
Issue date: August 28, 2026

Contents

1 About this guide

This guide describes how to install and manage Vault.

Revision information

See the table below for changes in each document issue.

Issue	Date	Section	Changes
1.0	Aug 2026	All	Document release

Other documentation

For instructions on using Vault, see:

https://api.managed.entrust.com/vaultaas

The options described apply to both on-premises and cloud-based product versions.

Documentation feedback

You can rate and provide feedback about product documentation by completing the online feedback form:

https://go.entrust.com/documentation-feedback

Any information you provide goes directly to the documentation team and is used to improve and correct the information in our guides.

2 About Cryptographic Security Platform

The Cryptographic Security Platform (CSP) software solution provides a unified platform for managing, protecting, and assessing cryptographic assets. CSP provides functionalities in the following categories:

- Compliance Management
- HSM Management
- Certificate Management
- Keys and Secrets Management
- File Encryption

Compliance Management

These capabilities assist with assessing and managing compliance of identified keys, secrets, and certificates with specified requirements. May be deployed in a clustered configuration and includes:

- **Compliance Manager**: A CSP component that provides **centralized visibility, compliance, and risk governance** of the enterprise's cryptographic assets. It connects data sources—such as vaults and security object repositories—from which it imports metadata about security objects (keys, secrets, and certificates), aggregates this information into a centralized inventory, and evaluates assets against compliance requirements.
- **Discovery**: A CSP feature for **asset discovery and data collection**, used to collect information about cryptographic assets so they can be brought under centralized visibility. Discovery operates through configuration-based scans, which can be run manually or on a schedule. Scan results integrate directly with Compliance Manager to populate the inventory of certificates, keys, and secrets.
- **Standard Compliance Packs**: Pre-configured collections of compliance requirements designed to assist organizations in assessing cryptographic assets against commonly adopted industry standards and best practices.
- **Third-party Objects**: An optional functionality that allows metadata for keys, secrets, or certificates not created or stored directly by CSP components or Entrust's non-CSP Certificate Authority ("ECA") software to be imported into the Compliance Manager inventory. Imported third-party objects are included in compliance assessments and reporting but remain externally managed.

HSM Management

Provides centralized management, monitoring, and visibility for Entrust HSMs. It is deployed as part of the Compliance Management configuration and includes:

- **KeySafe 5:** Centralized management of Entrust HSMs (Security Worlds, card sets, soft cards, firmware, host applications) with cryptographic asset visibility via Compliance Manager.
- **KeySafe 5 Monitoring**: Optional capability for centralized monitoring of Entrust HSMs with live and historical health, performance, alerts, and utilization metrics.

Certificate Management

CSP optional add-on capabilities for deploying Public Key Infrastructure (PKI) functionality in clustered configurations, with usage limitations depending on the purchased license packages:

- **Certification Authority Package, includes:**
  - **Certificate Authority** solution providing certificate issuance, management, and validation, with built-in RESTful APIs for the CAs created and managed within the CSP.
  - **Certificate Enrollment Gateway** (CEG): a collection of certificate enrollment protocols. In this package, CEG may only be used for certificates created and managed within CSP.

- **Advanced PKI Package, includes**:
  - **Timestamping Authority**: software to prove that data existed at a specific time.
  - **Validation Authority**: certificate validation (OCSP) software specifically for (non-CSP) ECA.
  - **CA Gateway**: software consisting of RESTful APIs for integrating CAs. In this package, CA Gateway may only be used to integrate CSP with ECA.
- **Advanced CLM Package, includes**:
  - **Certificate Manager (formerly Certificate Hub)**: Certificate lifecycle management and automation across CAs created and managed within the CSP and third-party CAs, excluding CA functionality.
  - **CA Gateway**: In this package, it is permissible to use CA Gateway for integration with CSP CAs and non-CSP CAs.
  - **Certificate Enrollment Gateway**: In this package, it is permissible to use Certificate Enrollment Gateway for certificates created by both CSP and non-CSP CAs.

Keys and Secrets Management

CSP optional add-on capability for deploying multiple vault appliances in active-active Vault Clusters. Appears on Orders as "Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults." A Vault Cluster is a secure CSP software component that provides an isolated environment for managing cryptographic keys, secrets, and related objects. Vault Clusters securely generate, store, protect, and control access to cryptographic material while enforcing strong security controls and auditability.

Each Vault Cluster can manage one or more of the following vault types:

- **Vault for KMIP Keys**: Cryptographic keys, secrets, and certificates managed using the Key Management Interoperability Protocol (KMIP), enabling standardized and interoperable key lifecycle management across heterogeneous environments and applications.
- **Vault for Cloud Keys**: Encryption keys used in cloud key management services—such as AWS KMS, Azure Key Vault, and Google Cloud KMS—to protect cloud-native workloads and data. CSP supports bring-your-own-key (BYOK), hold-your-own-key (HYOK), and native key management models, depending on the target cloud service.
- **Vault for Secrets**: Sensitive data such as passwords, API keys, access tokens, and credentials that require secure storage, access control, and lifecycle management.
- **Vault for Application Keys**: Cryptographic keys used by applications to perform cryptographic operations—such as encryption, digital signatures, and hashing—via CSP cryptographic APIs or command-line interfaces.
- **Vault for TDE Database Keys**: Encryption keys used to protect databases with Transparent Data Encryption (TDE), including Oracle, Microsoft SQL Server, MariaDB, and open-source PostgreSQL, ensuring data at rest is encrypted.
- **Vault of Virtual Machine Encryption Keys:** Cryptographic keys used to encrypt Windows and Linux virtual machine operating system disks and attached data volumes in virtualized environments.

File Encryption

File Encryption is a CSP software component that encrypts file-based data and may be deployed in a clustered configuration. File Encryption supports both:

- Software-based encryption, where hardware HSM protection is not required, and
- Hardware-based encryption, leveraging Entrust HSMs for enhanced key protection.

The File Encryption capability includes 10 GB of protected data capacity. Additional encrypted data capacity may be added by purchasing 1 TB add-on annual subscriptions.

3 About CSP Vault

Major Components

Entrust Cryptographic Security Platform Vault® provides encryption and key management for virtual machines located in data centers or private, public, or hybrid clouds. Entrust Cryptographic Security Platform Vault works with:

- VMware vSphere
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

Entrust Cryptographic Security Platform Vault consists of two main components:

- **Entrust Cryptographic Security Platform Vault** (CSP Vault)—CSP Vault stores encryption keys, policies, and configuration for any number of virtual machines with the Entrust Policy Agent installed. You can configure CSP Vault directly through one of the browser-based webGUIs using HTTPS, or remotely through the `hicli` command line interface (CLI) or a set of REST-based APIs.

  You can install multiple CSP Vault nodes in an active-active cluster to provide load balancing and high availability support. Because this is an active-active cluster, you can make changes to the settings on any CSP Vault node in the cluster and those changes are immediately reflected on all CSP Vault nodes in the cluster.

- **Entrust Policy Agent** (Policy Agent)—A software module that runs inside Windows and most Linux operating systems that provides encryption of virtual disks, filesystems, and individual files. All VMs that have the Policy Agent installed can also securely share encrypted files and disks as long as those VMs are registered with the same Cloud VM Set.

  You must install a copy of the Policy Agent on each VM that you plan to use with the CSP Vault for Databases or the CSP Vault for VM Encryption.

Entrust Hardened OS

The base of every Cryptographic Security Platform Vault node is the Entrust-hardened version of Oracle Linux, a locked-down version of the operating system that has no run-time login/SSH access to the system. This prevents tampering or attempts to access clear-text data and/or encryption keys. Each Cryptographic Security Platform Vault node can be installed as a virtual machine.

The main features are:

- An ISO, OVA, AMI (Amazon Web Services marketplace), VHD (Microsoft Azure marketplace), or Google Cloud Platform Image that supports installation of a Cryptographic Security Platform Vault node, from which the Entrust Policy Agent can be downloaded.
- Optional automatic mirroring of the root partition to provide high availability for CSP Vault servers, preventing downtime from disk failures.
- Encryption of the Entrust software on the installation media, to prevent tampering.

- All major system software protected from tampering by whitelisting.
- No login or SSH access to CSP Vault, preventing key snooping or clear-text data snooping.
- Minimal OS software installed with industry standard lock-down capabilities built in.
- Ability to extract debug information via the webGUI or through a restricted support access. The debug information does not contain any sensitive data or encryption keys.
- GUI-based extraction of log / support information.
- Built-in VMtools.

CSP Vault Clusters

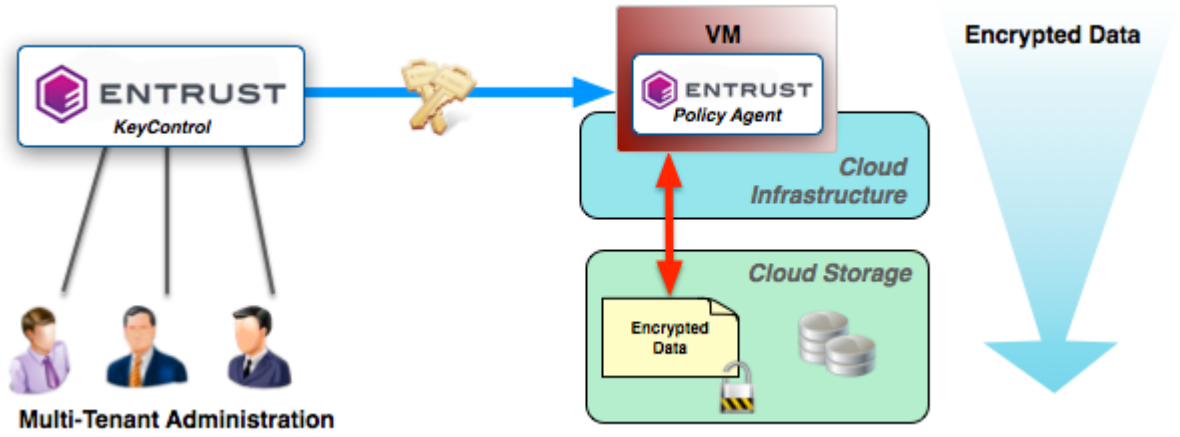
At the heart of every Entrust Cryptographic Security Platform Vault deployment is an active-active cluster of Cryptographic Security Platform Vault nodes that manage encryption keys for virtual Linux and Windows machines.

CSP Vault features include:

- An active-active cluster for high availability. Any changes made to any Cryptographic Security Platform Vault node in the cluster are automatically reflected on all nodes in the cluster.
- Clustered object store protecting keys, policies and configuration data. All objects are encrypted and ultimately wrapped with an Admin Key.
  The Admin Key uses a software-based "n of m" backup. This prevents Cryptographic Security Platform Vault backups from being stolen and installed on new hardware.
- Nodes can join or leave the cluster without affecting Cryptographic Security Platform Vault's ability to deliver encryption keys.
- A Cryptographic Security Platform Vault cluster moves into degraded mode (read only) on network disconnect or failure. While in degraded mode, any Cryptographic Security Platform Vault node can still serve requests for existing keys and policies from VMs where the Policy Agent is installed. However, new encryption keys cannot be created.
- Each Policy Agent communicates with any Cryptographic Security Platform Vault node, switching between them if they detect a non-responsive Cryptographic Security Platform Vault node.
- All system components of the Cryptographic Security Platform Vault are encrypted.
- Support for admin authentication via local accounts with strict password controls or via accounts stored in LDAP (including Microsoft AD).
- Support for Alerts in environments with and without email access.
- Full-featured command line utilities (`hicli` and `hcl`).
- A rich RESTful API.

About Entrust Policy Agent

The Entrust Policy Agent provides for encryption of disks, filesystems and files within a virtual machine.



There are a number of features provided in the Policy Agent, including:

- Full encrypted path from the VM, through the hypervisor to the storage.
- Support for cloning and replication.
- Dynamic rekey on Windows and Linux, allowing initial encryption or rekey without taking the VM or applications offline.
- Filesystem resize for encrypted devices.
- Support for Amazon S3 storage.
- Linux file-level and folder-level encryption.
- Migration of encrypted disks between VMs in the same Cloud VM Set.
- Support for Windows failover clusters.
- Root and swap encryption for Linux and boot drive (C:) encryption for Windows.

This section includes:

- Encryption Key Sizes and Algorithms
- Secure File Migration

Encryption Key Sizes and Algorithms

You can specify a specific cipher type when disks are encrypted or when KeyIDs are created. By default, the Policy Agent uses AES-XTS-512 encryption to take advantage of the performance improvements that come with AES-NI (Advanced Encryption Standard New Instructions).

Policy Management encryption keys:

- Support AES and AES-XTS encryption. Specifically:

Algorithm	Mode	Notes
AES-128	CBC	Available *only* for KeyIDs. Not available when encrypting Linux or Windows disks. Uses a single 128-bit encryption key.

Algorithm	Mode	Notes
AES-256	CBC	Uses a single 256-bit encryption key.
AES-XTS-256	XTS	Not available on Windows boot drives. Uses a pair of 128-bit encryption keys.
AES-XTS-512	XTS	Uses a pair of 256-bit encryption keys, one data AES key and one tweak AES key. The IV is generated using aes-xts-essiv:sha256.
AES-XTS-512-FIPS	XTS	Uses a pair of 256-bit encryption keys, one data AES key and one tweak AES key. The IV is generated using aes-xts-plain64, which is approved by FIPS.

- Automatically detect and use hardware cryptography—AES-NI on Intel and AMD processors.
- Can be assigned an expiration date—one key per device is generated.
- Enable secure encrypted communication between Cryptographic Security Platform Vault clusters and Policy Agents.
- Allow users to revoke or restore access to all keys for a VM.
- Allow users to cache keys in the VM (encrypted with a passphrase).
- Allow users to clone VMs and authenticate cloned VMs (for backup, restore, autoscaling, and DR purposes).
- Enable the Policy Agents to share encryption keys and disks between VMs in the same Cloud VM Set, which allows these VMs to encrypt, securely transport, and decrypt data and disks.
- Allow users to rekey both Windows and Linux disk while those disks are online and accessible.
- The FIPS certified version uses the key size designation in the name instead of the overall key material size.

AES-NI is supported by all current-generation EC2 instances in Amazon Web Services (AWS) and by all Microsoft Azure instances. To check whether a specific server supports AES-NI, run `hcl status` on the server or look at the VM details in the Cryptographic Security Platform Vault webGUI under Cloud > VMs.

For additional details about AES-NI, see the Wikipedia summary at http://en.wikipedia.org/wiki/AES_instruction_set.

Secure File Migration

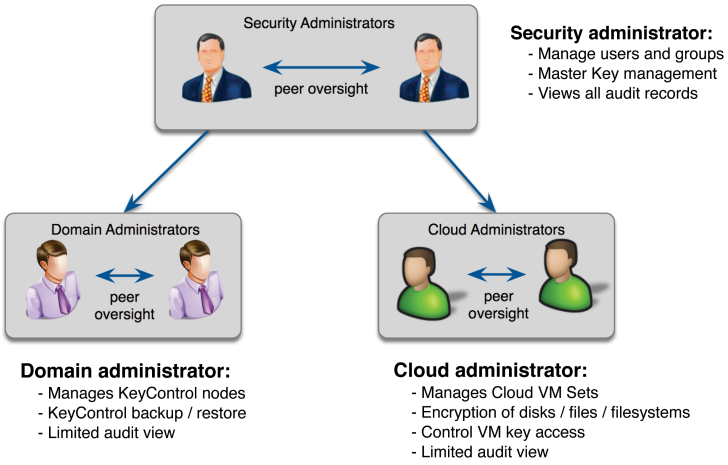
In VMs with the Policy Agent installed, we support the ability to share KeyIDs (encryption keys referenced by a symbolic name) between VMs within the same Cloud VM Set in which the KeyIDs were created. This allows you to encrypt files and move them securely between these VMs. Only the VMs within the same Cloud VM Set as the KeyIDs are able to decrypt the files. Encryption is on a file-by-file basis, so movement of larger amounts of data can be achieved by zipping/tarring groups of files and then encrypting them.

These mechanisms can also be used to encrypt files and move them to cloud storage knowing that only you will be able to decrypt the files on return.

As an extension to the KeyID notion, we also provide interfaces for migrating encrypted files between VMs and through Amazon Web Services (AWS) S3 storage.

Administrative Model

Entrust Cryptographic Security Platform Vault provides a rich administrative framework that can be leveraged by multiple organizations of different sizes. This approach is useful for organizations ranging from the single-administrator IT shop to a large, multi-tenant cloud service provider who needs to support secure customer environments.



The administration model provides:

- Multi-tenancy support. Administrative roles allow for need-to-know and separation of duties. There are three distinct administrative roles (Security, Domain, and Cloud). Roles can be combined and there are no limits to the number of administrators. Administrators can be placed in administrative groups to provide peer oversight. All objects in the system are owned by one or more administrative groups, not by individual administrators.
- Support for multiple administrative roles per admin.
- Alerts presented through the Cryptographic Security Platform Vault webGUI and, optionally, sent through email.
- Audit records that can be displayed in the Cryptographic Security Platform Vault webGUI, downloaded, or exported through syslog to an external log server.

Administrative Interfaces

Entrust provides several administrative interfaces that allow you to configure and maintain Cryptographic Security Platform Vault and the encrypted VMs registered with Cryptographic Security Platform Vault.

Interface	Description
Cryptographic Security Platform Vault webGUI	A browser-based HTTPS interface to Cryptographic Security Platform Vault that lets you perform Cryptographic Security Platform Vault configuration and VM management. You can log into the webGUI on any Cryptographic Security Platform Vault node in the cluster. Any changes you make on that node are automatically disseminated to all other Cryptographic Security Platform Vault nodes in the cluster. For more information, see CSP Vault Management webGUI Overview.
Entrust Cryptographic Security Platform Vault System Console	The Entrust Cryptographic Security Platform Vault System Console is available on each Cryptographic Security Platform Vault node in the cluster. It lets you set local configuration options for the node and perform basic functions such as joining the node to an existing Cryptographic Security Platform Vault cluster and managing support access to the node. For more information, see CSP Vault System Console Overview.
`hicli`	CLI (command line interface) commands that allow you to configure and maintain both Cryptographic Security Platform Vault and the VMs registered with Cryptographic Security Platform Vault. For more information, see hicli Scripting Guide.
Entrust Policy Agent GUI	A Windows-only GUI installed with the Entrust Policy Agent. The Entrust Policy Agent GUI allows you to register and authenticate the VM on which it is installed. It also lets you encrypt and decrypt the disks on that VM. Unlike the other interfaces, the Entrust Policy Agent GUI is limited to the VM on which it is installed. You cannot use the Entrust Policy Agent GUI on one VM to manage the disks on a different VM, even if both VMs are registered with Cryptographic Security Platform Vault. For more information, see Entrust Policy Agent GUI Overview.
REST or Python APIs	Cryptographic Security Platform Vault can be configured and maintained through REST-based or Python-based API calls. The API documentation is located at https://<IP-Address>/apidoc/.

- CSP Vault Management webGUI Overview
- CSP Vault System Console Overview
- Entrust Policy Agent GUI Overview

CSP Vault Management webGUI Overview

When you configure a Cryptographic Security Platform Vault Management cluster, you assign each node in the cluster a static IP address. When you navigate to one of those static IP addresses in a web browser, Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. The Cryptographic Security Platform Vault Management webGUI lets you

configure Cryptographic Security Platform Vault Management appliance and manage the VMs registered with the cluster.

You can log into the Cryptographic Security Platform Vault Management webGUI on any Cryptographic Security Platform Vault node in the cluster and the changes will be automatically disseminated to all nodes in the cluster.

> Note: You should always explicitly log out of the Cryptographic Security Platform Vault Management webGUI when you are finished. If you close the browser without logging out first, Cryptographic Security Platform Vault keeps your session active until the Session Timeout is reached. For details, see Setting the CSP Vault Management webGUI Session Timeout.

The main features of the Cryptographic Security Platform Vault webGUI are:

- A Top Menu Bar that provides access to the main Cryptographic Security Platform Vault features. The icons you see in this bar depend on the user privileges associated with your account.
- A User menu next to the Top Menu Bar that lets you set your user preferences, log out from the webGUI, or open the product online help. The **Help** link in this menu is context-sensitive, so the help page displayed when you select this link depends on the currently-displayed page in the webGUI.
- A Dashboard that gives you an overview of your VMs in one place. For details, see Using the Dashboard.
- A **Refresh** button that allows you to control when the webGUI fetches updates from the network.

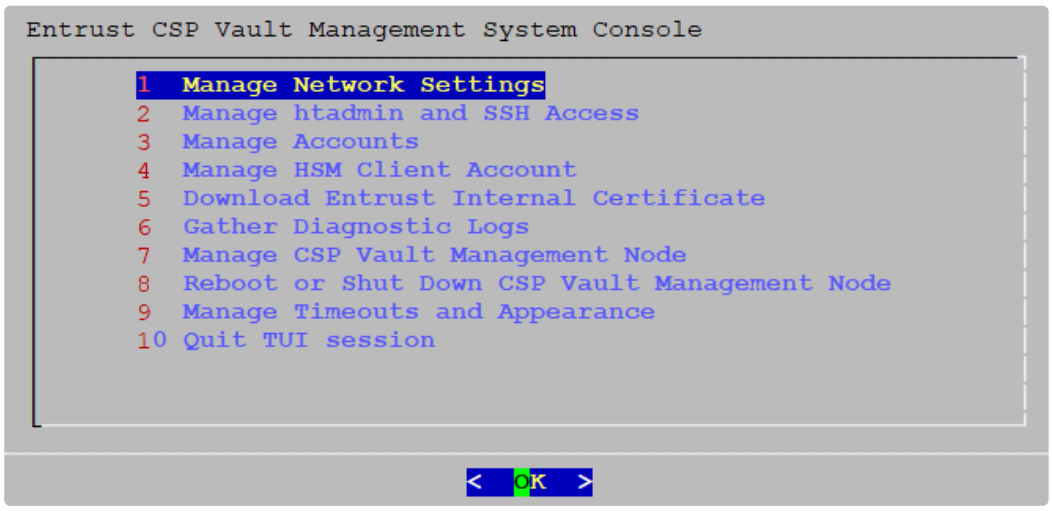
For all tables in the webGUI, you can:

- Display additional information for any object by clicking on that object.
- Sort by any column by clicking the column header.
- Select which columns are displayed by clicking the **Column Display Options** button.
- Toggle multi-select mode by clicking the **Multi-Select** button. If you have multiple objects selected, any action you take is applied to all selected objects.

For information about logging into the webGUI for the first time, see Initializing the CSP Vault Management webGUI. For information about administering Cryptographic Security Platform Vault using the webGUI, see Cryptographic Security Platform Vault System Configuration.

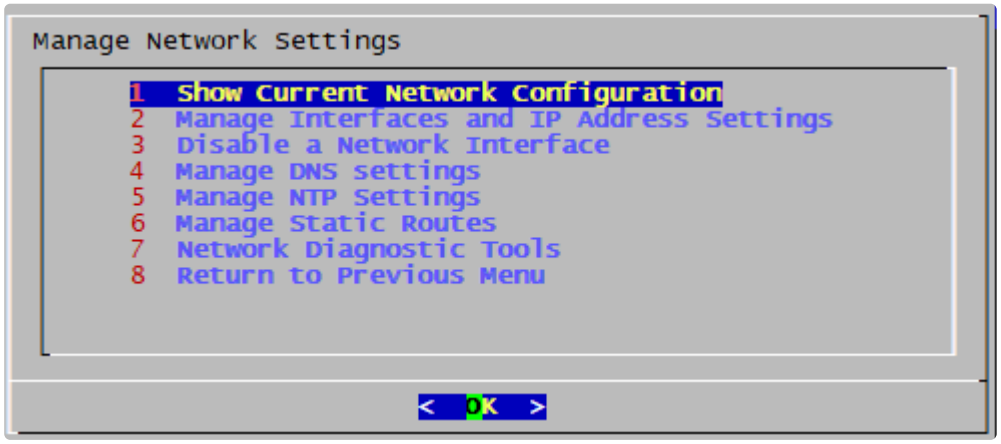
CSP Vault System Console Overview

When you log into the Cryptographic Security Platform Vault VM console as `htadmin`, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. This menu lets you configure the local Cryptographic Security Platform Vault server. In general, the changes you make here do not apply to any other Cryptographic Security Platform Vault node in the cluster.



The menu is a TUI (Text-based User Interface). You navigate through the TUI using the Tab key to move between fields and pressing Enter when the correct choice is highlighted. If the TUI screen has numbers at the start of the line, you can also press the corresponding number key and then press Enter to navigate through the menus.

In the screenshot above, pressing Enter goes to the Manage Network Settings screen of the TUI.

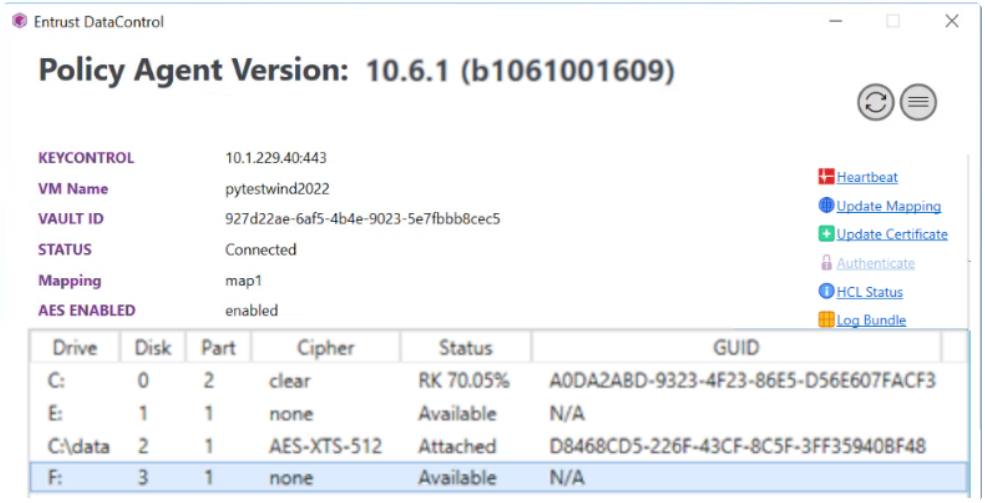


To return to the main Entrust Cryptographic Security Platform Vault System Console screen, press Esc (Escape). Based on where you are in the menus, you may need to press Esc several times.

For more information, see Using the Entrust CSP Vault System Console.

Entrust Policy Agent GUI Overview

The Entrust Policy Agent GUI is installed locally on the Windows server with the Entrust Policy Agent. It provides basic encryption, decryption, and rekeying functionality by sending requests to the CSP Vault for VM Encryption so that you do not need to log into the CSP Vault for VM Encryption webGUI.



The Entrust Policy Agent GUI allows you to register or authenticate the VM with CSP Vault for VM Encryption, and it displays the following information:

- the connection information.
- the status of each disk or folder mount on the VM.

In the Policy Agent,you can click the Heartbeat button to manually force a heartbeat connection, click the Update Mapping button to use the mapping that you created in the CSP Vault for VM Encryption webGUI, or right-click any of the listed disks or folder mounts to encrypt or decrypt them. In the screenshot above, the GUI shows that the folder mount `C:\data` is encrypted and attached to the CSP Vault for VM Encryption while `C:` is being encrypted and the encryption process has completed 70.05% of the disk.

If you had not yet registered the Policy Agent, then the screen would show a Register button that you can click to register it.

For details, see Windows Encryption Management with the Entrust Policy Agent GUI.

4 Release notes

The following changes were made in past Cryptographic Security Platform Vault releases.

For details about the current Cryptographic Security Platform Vault release and previous releases, visit trustedcare.entrust.com. If you do not have a login, please contact trustedcaresupport@entrust.com.

Changes in Release 10.5.3

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.6.1 from versions 10.5.1 and 10.5.3. For the Entrust Policy Agent, you can upgrade to 10.5.1 from versions 10.4.5, 10.4.7, 10.5.1, and 10.5.3.

Changes in this release:

- You can now encrypt multiple databases with one command.
- If you use geographically distributed nodes in your cluster and have performance issues, you can switch your master node to the server closest to where most data is generated.
- You can now choose which node will become the master node after the master node is removed from the cluster.
- You can now choose whether or not you want to enable audit logging for HYOK, EKM, and XKS operations at the Key Set level.

Changes in Release 10.5.1

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.5.1 from versions 10.4.3, 10.4.5, and 10.4.7. For the Entrust Policy Agent, you can upgrade to 10.5.1 from versions 10.4.3, 10.4.5, and 10.4.7.

Changes in this release:

- Licenses are now enforced in the Cryptographic Security Platform. You will see pop-up warnings in the webGUI when there are important license issues.
- Expanded support for Post-Quantum Encryption and Key Management, including support for ML-KEM, ML-DSA, and SLH-DSA keys, as well as encapsulation, decapsulation, sign, and verify operations using these keys. Also added improved PQ security for KMIP Server with support for PQ-TLS.
- You can now use KeySafe5 (part of the CSP appliance) to monitor your nShield HSM when configured with the Cryptographic Security Platform Vault.
  Note: You can view the KeySafe5 GUI through the Cryptographic Security Platform Compliance Manager.

- Azure updates including Multi-Vault keys and the ability to manage multiple Azure
- The Cryptographic Security Platform Vault for Cloud Keys now supports on-demand key rotation for AWS key versions with BYOK.
- The Cryptographic Security Platform Vault for Secrets now supports Microsoft SQL Server
- The Cryptographic Security Platform Vault for Secrets now supports EnterpriseDB Postgres.
- Added the Batch Encrypt, Batch Decrypt, and Batch encrypt-decrypt API and CLI commands in the Cryptographic Security Platform Vault for Cryptographic APIs.
- Added support for OCI users in non-default identity
- Added Authentication Inheritance, which enables Security Administrators to configure the Cryptographic Security Platform Vault Appliance with AD, OIDC, or OIDC with AD Authentication, and allows Vault Administrators to inherit that configuration in their vaults.
- Added the ImportClearKey API command in the Cryptographic Security Platform Vault for Cryptographic
- Made multiple enhancements to the Windows Policy Agent GUI, including support for TLS 3, increased launch speed, and reduced application size. You also have the ability to update mapping, perform encryption tasks on the drives, and view encryption details.

Changes in Release 10.4.7

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.4.7 from versions 10.4.1, 10.4.1.1, 10.4.3, and 10.4.5. For the Entrust Policy Agent, you can upgrade to 10.4.7 from versions 10.3.1, 10.3.3, 10.4.1, 10.4.1.1, 10.4.3, and 10.4.5.

Changes in this release:

- The Cryptographic Security Platform Vault for Secrets now supports AWS user credential secrets.
- The Cryptographic Security Platform Vault for Secrets now supports Postgres secrets.
- Added support for EnterpriseDB (EDB) PostgreSQL Advanced Server.
- Added support for AD groups.
- Added mTLS authentication support for the Cryptographic Security Platform Vault for Cryptographic APIs and the Cryptographic Security Platform Vault for Secrets.

Changes in Release 10.4.5

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.4.5 from versions 10.4.1, 10.4.1.1, and 10.4.3. For the Entrust Policy Agent, you can upgrade to 10.4.5 from versions 10.3.1, 10.3.3, 10.4.1, 10.4.1.1, and 10.4.3.

Changes in this release:

- KeyControl and KeyControl Compliance Manager have changed names.
    - KeyControl is now known as Cryptographic Security Platform Vault.
    - KeyControl Compliance Manager is now known as Cryptographic Security Platform Compliance Manager.
    - The KeyControl Vault for Application Security is now known as the Cryptographic Security Platform Vault for Cryptographic APIs.
- If a CloudKey's cloud status is unavailable, you can remove it immediately using the Force Purge command.
- You can now use certificate-based authentication with Azure BYOK.
- You can now use BYOK and cache-only keys (HYOK) with Salesforce.
- You can set up an automatic synchronization schedule to import all CloudKeys in a Key Set.
- You can now cache your keys in the Cryptographic Security Platform Vault for Cryptographic APIs.
- The Cryptographic Security Platform Vault for Secrets now supports Terraform secrets.
- Cryptographic Security Platform Vault for Databases now supports column-level encryption for PostgreSQL.
- You can now use mTLS authentication in the Cryptographic Security Platform Vault for Cryptographic APIs.

Changes in Release 10.4.3

Upgrade Path: For KeyControl, you can upgrade to 10.4.3 from versions 10.3.1, 10.3.3, 10.4.1, and 10.4.1.1. For the Policy Agent, you can upgrade to 10.4.1 from versions 10.3.1, 10.3.3, 10.4.1, and 10.4.1.1.

Changes in this release:

- You can now use BYOK with Oracle Cloud Infrastructure (OCI).
- You can now assign API users the BACKUP_USER role, which lets them manage backups but does not grant any other admin privileges.

Changes in Release 10.4.1.1

Release 10.4.1.1 is a cumulative release containing bug fixes and all new features from 10.4.1.

Upgrade Path: For KeyControl, you can upgrade to 10.4.1.1 from versions 10.3.1, 10.3.3, and 10.4.1. For the Policy Agent, you can upgrade to 10.4.1.1 from versions 10.3.1, 10.3.3, and 10.4.1.

Changes in Release 10.4.1

Version 10.4.1 is the first KeyControl release on Oracle Linux. The transition from CentOS to Oracle Linux allows Entrust to improve the security of the KeyControl operating system.

The main KeyControl components were ported directly to Oracle Linux and will continue to work as they did in earlier releases. The same applies to the KeyControl APIs.

Upgrade Path: For KeyControl, you can upgrade to 10.4.1 only from version 10.3.1. For the Policy Agent, you can upgrade to 10.4.1 from version 10.3.1.

Changes in this release:

- Entrust KeyControl now runs on the Entrust-hardened version of Oracle Linux.
- You can now use OpenID Connect (OIDC) Authentication with Active Directory in the KeyControl Vault Management appliance.
- You can now use OpenID Connect (OIDC) Authentication without configuring Active Directory in the KeyControl Vault Management appliance.
- AWS multi-Region keys are AWS KMS keys in different AWS Regions that can be used interchangeably. The KeyControl Vault for Cloud Keys now supports using AWS multi-region keys in BYOK.
- The KeyControl Vault for Cloud Keys now supports Azure role-based access control (Azure RBAC) and the access policy model authorization system.
- You can now use secondary approval with the KeyControl Vault for Secrets.
- You can now use Personal Access tokens in your KeyControl Vaults that use OIDC for authentication as a password for API and CLI commands.
- Added support for TLS 1.3 and Extended Master Secret (TLS). TLS 1.3 is the default for all new KeyControl installations.
- You can now set KeyControl to use self-signed certificates for all nodes in a cluster.
- The KeyControl appliance AMI now only supports Instance Metadata Service (IMDS) version 2 for AWS Cloud.

Changes in Release 10.3.1

Version 10.3.1 lays the groundwork for the upgrade to version 10.4.1, the first release of Cryptographic Security Platform Vault on Oracle Linux. The transition from CentOS to Oracle Linux allows Entrust to improve the security of the Cryptographic Security Platform Vault operating system, but it also requires a different migration path than previous Cryptographic Security Platform Vault upgrades.

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.3.1 from version 10.2. For the Entrust Policy Agent, you can upgrade to 10.3.1 from versions 10.2, 10.1.1, and 10.1.

Changes in this release:

- You can now use OpenID Connect (OIDC) Authentication without configuring Active Directory in your individual KeyControl vaults.
- You can now use Active Directory (AD) or OpenLDAP for authentication in the KeyControl Vault Management appliance.
    - AD users are supported, but not AD groups.
    - Two-factor authentication is supported for local users only.

Changes in Release 10.2

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.2 from versions 10.1 and 10.1.1. For the Entrust Policy Agent, you can upgrade to 10.2 from versions 10.1 and 10.1.1.

Changes in this release:

- You can now use hardware security modules with the Cryptographic Security Platform Vault for Secrets.
- You can now use BYOK with GCP in the Cryptographic Security Platform Vault for Cloud Keys.
- You can now use MariaDB with TDE in the Cryptographic Security Platform Vault for Databases.
- You can now use the HTTPS proxy server with BYOK for AWS and Azure.
- Support for Double Key Encryption for Microsoft 365 in the Cryptographic Security Platform Vault for Cloud Keys.
- Two-Factor Authentication is now offered with each Cryptographic Security Platform Vault.

Changes in Release 10.1.1

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.1 from versions 10.0 and 10.1. For the Entrust Policy Agent, you can upgrade to 10.1 from versions 10.0 and 10.1.

Changes in this release:

- You can now upgrade KeyControl version 10.0 to KeyControl Vault 10.1.1.
- You no longer need to enable (SMTP) in the Appliance Manager UI when adding KeyControl Vaults. This restriction was removed in the 10.1 release.
- KeyControl Vault PASM vaults now support Ansible.

Changes in Release 10.1

Upgrade Path: You can only deploy Entrust Cryptographic Security Platform Vault 10.1 as a new installation. Upgrading from previous versions of Entrust Cryptographic Security Platform Vault is not supported.

Changes in this release:

- New Entrust Cryptographic Security Platform Vault Architecture. The Entrust Cryptographic Security Platform Vault family of products has been divided into two components:
    - Cryptographic Security Platform Compliance Manager—This application handles all global requirements for your vaults, such as licensing and authorization.
    - Entrust Cryptographic Security Platform Vault—All of the Entrust Cryptographic Security Platform Vault applications have been separated and moved into individual vaults.
- You manage licensing for all Entrust Cryptographic Security Platform Vaults using Cryptographic Security Platform Compliance Manager.

- You can now use Cryptographic Security Platform Vault as an external key manager (EKM) provider for Oracle Server.
- You can now use Cryptographic Security Platform Vault as an AWS KMS External Key Store (XKS).
- You can now use the new Tokenization Vault and APIs for tokenization, masking, and data encryption.
- You can now use Cryptographic Security Platform Vault with Azure-managed HSMs.
- You can now configure Syslog Server to use ArcSight Common Event Format (CEF) for logging.
- Cryptographic Security Platform Vault now supports Remote Administration Ready Smartcards for nShield HSMs.
- Cryptographic Security Platform Vault now includes the Luna HSM library v10.5.1-174

Changes in Release 10.0

Upgrade Path: For Entrust Cryptographic Security Platform Vault, you can upgrade to 10.0 from versions 5.5 and 5.5.1. For the Entrust Policy Agent, you can upgrade to 10.0 from versions 5.3, 5.4, 5.5, and 5.5.1.

Changes in this release:

- You can now use Cryptographic Security Platform Vault as an EKM provider for Microsoft SQL.
- You can now use Cryptographic Security Platform Vault to manage your SSH keys.
- You can now use Bring Your Own Key (BYOK) with Google Cloud Platform.
- You can now use Cryptographic Security Platform Vault with nShield HSMs that are enrolled in FIPS 140 Level 3 Security Worlds.

5 Requirements

See below for the Vault requirements.

System resources

Entrust recommends the following system resources based on your installation size. If your system does not meet these requirements, the installation may fail, or you may encounter performance issues.

Resource	Standard installation	Large installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a large installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

Network requirements

All Cryptographic Security Platform Vault IP addresses must use IPv4. Cryptographic Security Platform Vault does not support IPv6 addresses.

For Cryptographic Security Platform Vault to Cryptographic Security Platform Vault, Cryptographic Security Platform Vault to Cryptographic Security Platform Compliance Manager, and Policy Agent to Cryptographic Security Platform Vault, the following ports need to be open:

- **Internal protocol**—The Cryptographic Security Platform Vault nodes must be able to communicate on `TCP/443`, `TCP/8443`, and `TCP/5432`. If you have a firewall between one or more nodes, make sure these ports are open.
- **Cryptographic Security Platform Compliance Manager**—The Cryptographic Security Platform Vault nodes must be able to communicate `TCP/443` outbound to the Cryptographic Security Platform Compliance Manager.
- **Cryptographic Security Platform Vault webGUI**—Inbound TCP/443 to administrator systems from any Cryptographic Security Platform Vault server in the cluster.
- **Cryptographic Security Platform Vault support-level access**—Inbound TCP/22 from administrator systems to any Cryptographic Security Platform Vault server in the cluster.
- **Policy Agent to Cryptographic Security Platform Vault**—Inbound TCP/443 from the Policy Agent to each of the Cryptographic Security Platform Vault nodes in the cluster.

For Cryptographic Security Platform Vault infrastructure services, the following ports need to be open:

- **DNS**—Outbound UDP/53
- **SMTP**—Outbound mail server, typically TCP/25.

  > If you disable SMTPS and the server supports StartTLS, it will use StartTLS when the connection is made. SMTPS is not compatible with StartTLS, and only one can be used.

- **SYSLOG**—An outbound TCP/UDP port between 25 and 65535 if you want to use a remote syslog server. Cryptographic Security Platform Vault supports both TCP and UDP for syslog.
- **Backup and Restore via NFS**—If you want to access the Cryptographic Security Platform Vault-generated backup files via NFS, you need to open the following ports: 2046 (lockd), 2047 (rpc statd), 2048 (rcp mountd), and 2049 (default NFS port).
  If you need to check the port status, you can run one of the following commands:
  `rcpinfo <KeyControl_Vault_IP_Address>` or `rcpinfo <KeyControl_Vault_Name>`
- **NTP**—Outbound NTP servers, typically UDP/123 or TCP/123

  > The network ports indicated for SMTP, syslog, and NTP are the typical ports for these services. If you need to change those ports, consult with the administrators of these services.

To configure Cryptographic Security Platform Vault as a KMIP server, open the port you plan to use. The default KMIP port is 5696.

Supported platforms

We support the 64-bit versions of the Linux and Windows platforms listed below. 32-bit versions are *not* supported.

- Hypervisors supported for Vault
- Linux platforms supported for Policy Agent
- Windows platforms supported for Policy Agent
- Hypervisors Supported for Policy Agent

> The following information is for virtual machines only. Physical servers are not supported.

Hypervisors supported for Vault

See below for the hypervisors supported for Entrust Cryptographic Security Platform Vault.

Hypervisor	Versions supported	Notes
KVM hypervisor	Red Hat 7.8 and above	To access the System Console in KVM on Redhat 10.0, please use the RHEL web console (Cockpit).
VMware ESXi	VMware ESXi 8.0 (HW version 20) and above	

Hypervisor	Versions supported	Notes
AWS	Latest Entrust version available in the marketplace	
Azure	Latest Entrust version available in the marketplace	
Google Cloud Platform	Latest Entrust version available in the marketplace	
Nutanix AHV	Nutanix AOS 7.3 and above	Documentation for deploying Entrust Cryptographic Security Platform on Nutanix is available on the nShield Documentation site. Search on Nutanix to locate it on the page.
Microsoft Hyper-V and Hyper-V 2025	Microsoft Windows Server 2019, 2022, 2025	

Linux platforms supported for Policy Agent

All supported Linux versions also support XFS (Extent File System). If the Linux version you are running is not listed, contact Entrust Support and provide information about the Linux version and the problems encountered.

Linux Online Encryption is only supported for RHEL 8.0 or later, or Ubuntu 20.04 or later. For details, see Linux Online Encryption Prerequisites and Considerations

Platform	Data encryption	Root/Swap encryption	Online encryption	Offline encryption
RHEL10.0 - 10.2	✓	✓	✓	✓
RHEL 9.0 - 9.8	✓	✓	✓	✓
RHEL 8.10	✓	✓	✓	✓
Ubuntu 26.4	✓	✓	✓	✓

Platform	Data encryption	Root/Swap encryption	Online encryption	Offline encryption
Ubuntu 24.04	✓	✓	✓	✓
Ubuntu 22.04	✓	✓	✓	✓
Rocky Linux 10.0 - 10.2	✓	✓	✓	✓
Rocky Linux 9.4 - 9.8	✓	✓	✓	✓
Rocky Linux 8.10	✓	✓	✓	✓
Oracle Linux 10	✓	✓	✓	✓
Oracle Linux 9.1 - 9.8	✓	✓	✓	✓
Oracle Linux 8.10 - 10.2	✓	✓	✓	✓
SUSE Linux Enterprise Server 15 SP7	✓	✓	✗	✓
SUSE Linux Enterprise Server 12 SP5	✓	✓	✗	✓

Windows platforms supported for Policy Agent

All Windows operating systems listed below are supported on Amazon Web Services and Microsoft Azure. For data encryption:

- Only Windows basic disks are supported. Windows dynamic disks are *not* supported.
- To use the `hicli` command line interface with Windows, you need to enable WinRM (Windows Remote Management), which is disabled by default. The Python `pywinrm` package must also be installed on the Windows control node on which `hicli` is running.

⚠ Make sure that you have the latest Microsoft patches on your Windows operating system.

Platform	Data drive and Folder encryption	Boot drive encryption	Online encryption
Microsoft Windows Server 2025 (OS build 26100) (UEFI Enabled)	✔	✔	✔
Microsoft Windows Server 2022 (OS build 20348)	✔	✔	✔
Microsoft Windows Server 2019 (OS build 17763)	✔	✔	✔
Microsoft Windows Server 2016 (OS build 14393)	✔	✔	✔
Server Core for Microsoft Windows Server 2019	✔	✔	✔
Server Core for Microsoft Windows Server 2016	✔	✔	✔

Hypervisors Supported for Policy Agent

Both Linux and Windows clients are supported with the following Hypervisors.

Hypervisor	Data encryption	Root/Swap and Boot Encryption
VMware ESXi 8.0 (HW version 20) and above	✔	✔
Microsoft Hyper-V	✔	✔
KVM (on RHEL 8 and above)	✔	✔
AWS	✔	✔
Azure	✔	✔
Google Cloud Platform	✔	✔
Nutanix AHV	✔	✔

Browser Requirements

The Cryptographic Security Platform Vault webGUI administrative interface requires HTTPS access and has been tested on the following browsers:

- Chrome
- Firefox
- Edge

6 Installing CSP Vault

Installation Overview

This document contains the standard installation procedures for Entrust Cryptographic Security Platform Vault.

- For installation on Amazon Web Services, see CSP Vault in Amazon Web Services.
- For installation on Microsoft Azure, see CSP Vault in Microsoft Azure.
- For installation on Google Cloud Platform, see CSP Vault in Google Cloud Platform.

To configure a basic Cryptographic Security Platform Vault cluster and register one or more VMs with that cluster, you need to install Cryptographic Security Platform Vault on one or more servers and then install the Policy Agent on each VM you want to register. To do so:

Step	Description	Notes
1	Verify that the systems you want to use meet the basic system requirements.	See Requirements.
2	Install the Cryptographic Security Platform Vault software on the target system. Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.	If you want to use VMware vCenter to deploy Cryptographic Security Platform Vault using an OVA template, see CSP Vault OVA Installation. If you want to install Cryptographic Security Platform Vault on an existing VM, see CSP Vault ISO Installation for Hypervisor.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	For OVA, see Configuring the First CSP Vault Node (OVA Install). For ISO, see Installing the First CSP Vault Node from an ISO Image.

Step	Description	Notes
4	If desired, install additional Cryptographic Security Platform Vault nodes and join them to the cluster. The number of nodes you can install is dictated by your Cryptographic Security Platform Vault license.	For OVA, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install). For ISO, see Installing a New Cryptographic Security Platform Vault Cluster Node from an ISO Image.

CSP Vault OVA Installation

OVA installation overview

For deployment in a vSphere environment with vCenter, Entrust provides a single virtual node in OVA format. You use the same OVA file to install as many Cryptographic Security Platform Vault nodes as you need.

> If you are running directly on ESX and not through vCenter, install from an ISO image as described in CSP Vault ISO Installation for Hypervisor.

Installing CSP Vault from an OVA Template

Before You Begin

Make sure that:

- You know the IP address and any required network connection information, such as the domain name and the DNS and gateway IP addresses, for the machine on which you are installing Cryptographic Security Platform Vault.
  Note: You must use an IPv4 address. Cryptographic Security Platform Vault does not support IPv6 addresses.
- You have the required permissions to install software on the target system.
- The target system meets the basic system requirements described in System Requirements.
- If you are using VMware, ensure that all of your CSP Vault deployments have VM-to-Host affinity enabled. This allows you to avoid Admin Key Recovery due to host migration. We recommend that you select 'Should run on hosts in group' for the rule specification. The group should contain only the one ESXi host that you are using for this Cryptographic Security Platform Vault VM.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Procedure

1. Log in to your vSphere Client.
2. Navigate to **Hosts and Clusters**.

3. Select **Actions > Deploy OVF Template**.
   Note: In this context, OVF and OVA are synonymous.
4. On the **Select template** page of the **Deploy OVF Template** wizard, browse to the location of your OVA file.
5. Select the file and click **Next**.
6. Specify the appropriate installation information in the remaining pages of the **Deploy OVF Template** wizard. Required fields are shown in red.
   On the **Select configuration** page, the configuration options use the following resources:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

   Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:
   - More than four nodes in the Cryptographic Security Platform Vault cluster.
   - More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
   - More than 100,000 secrets stored.

   Note: The OVA deployment method creates the disk as 60 GB, even for large configurations. After Cryptographic Security Platform Vault is configured, please follow the vSphere instructions on increasing the disk size and increase it to 140 GB. This will require a reboot of Cryptographic Security Platform Vault. You must increase the size for each node. For details, see Increasing CSP Vault Storage in a VM.

   On the **Customize template** page:
   - If you want to specify multiple DNS servers, enter their IP addresses as a comma-separated or space-separated list.
   - Specify a static IPv4 address in the **Host IP address** field. If you have an internal IP address that differs from your external IP address due to your firewall configuration, use the internal IP address. You *cannot* change the IP address for the node after it has been deployed.
     Note: You must use an IPv4 address. Cryptographic Security Platform Vault does not support IPv6 addresses.
   - Do *not* use spaces or special characters in the **Hostname** and **Domain Name** fields. Only use alphanumeric characters or hyphens (-). You *cannot* change the hostname after the node has been deployed.
     Note: Any uppercase letters in the hostname will be translated to lowercase after the node has been deployed.

   For information about the other fields in this wizard, see your vSphere Client documentation.
7. After you have finished entering the deployment information, click **Next** and review your choices on the **Ready to complete** page.
8. Click **Finish** to deploy the Cryptographic Security Platform Vault node.
9. Wait until you receive a message that the installation is complete.
   You can view the installation progress in the **Recent Tasks** tab in the vSphere Client.
10. If you selected the large installation configuration earlier in this procedure, you need to manually change the disk size allotted to the VM from the standard 65 GB to 150 GB. The OVA template sets the appropriate number of CPUs and the memory allocation but it *cannot* automatically change the standard disk size.
11. Power on the Cryptographic Security Platform Vault VM.

12. Configure the node as needed. For details, see one of the following:
    - If this is the first Cryptographic Security Platform Vault node in the system or if you want this to be a standalone node, follow the steps in Configuring the First CSP Vault Node (OVA Install).
    - If you are adding this node to an existing Cryptographic Security Platform Vault cluster, follow the steps in Adding a New CSP Vault Node to an Existing Cluster (OVA Install).

Configuring the First CSP Vault Node (OVA Install)

This procedure explains how to use this console to configure this system as the first Cryptographic Security Platform Vault node in the system. If you want to join this node with an existing Cryptographic Security Platform Vault node, see Adding a New CSP Vault Node to an Existing Cluster (OVA Install).

1. Log into the system on which you installed the Cryptographic Security Platform Vault software.
   The Cryptographic Security Platform Vault installer will automatically start running as soon as the VM is powered on.
2. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.

The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.

1. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the login prompt.
2. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
   a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
   b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
      Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
   c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
   d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
   e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
   f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
   g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.

If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.

h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install).
- To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

Adding a New CSP Vault Node to an Existing Cluster (OVA Install)

When you log into the target system for the first time after installing the Cryptographic Security Platform Vault software, Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault System Menu. This procedure explains how to use this menu to configure this system as a new node in an existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If Startup Authentication is enabled, you cannot add a new Cryptographic Security Platform Vault node. You must disable Startup Authentication on the existing Cryptographic Security Platform Vault node, add the new node, and then re-enable Startup Authentication.

Procedure

1. Log into the VM on which you installed the Cryptographic Security Platform Vault software.
2. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
3. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address you specified during installation. For security reasons, you must explicitly specify `https://` in the URL.

Tip: If you do not know the Management IP address for the node, log into the system on which the node is installed as `htadmin`. Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. From the menu, select **Manage Network Settings > Show Current Network Configuration**.

4. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
5. On the **Entrust Cryptographic Security Platform Vault Login** page, enter `secroot` for both the username and password.
6. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
7. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
8. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
9. Click **Continue**.
10. On the Download CSR page, click **Generate and Download CSR**.
11. Click **Continue**.
12. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
13. Select **Actions > Add a Node**.
14. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
15. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
16. Click **OK** to close the Add a Node window.
17. Return to the new node and click **Continue**.
18. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
19. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
20. When the node has successfully restarted, click **Login**.

What to Do Next

To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

CSP Vault ISO Installation for Hypervisor

ISO Installation Overview

Entrust provides an ISO image that allows you to install the first Cryptographic Security Platform Vault node or add a Cryptographic Security Platform Vault node to an existing cluster.

If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.

> Note: If you want to deploy Cryptographic Security Platform Vault using an OVA template, see CSP Vault OVA Installation.

Installing the First CSP Vault Node from an ISO Image

This procedure describes how to use the Entrust-provided ISO image to install and configure a standalone Cryptographic Security Platform Vault node or the first node in new Cryptographic Security Platform Vault cluster. If you want to add a Cryptographic Security Platform Vault node to an existing cluster, see Installing a New CSP Vault Cluster Node from an ISO Image.

If you want to deploy the node from an OVA template, see Installing CSP Vault from an OVA Template.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Before You Begin

- If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.
- Make sure that the target VM can access the Entrust Cryptographic Security Platform Vault ISO image.
- Make sure the target VM meets the basic system requirements described in Requirements.
- If you are using VMware, ensure that all of your CSP Vault deployments have VM-to-Host affinity enabled. This allows you to avoid Admin Key Recovery due to host migration. We recommend that you select 'Should run on hosts in group' for the rule specification. The group should contain only the one ESXi host that you are using for this Cryptographic Security Platform Vault VM.

Procedure

1. Log into the vSphere Client.
2. Create a new virtual machine using the settings appropriate to your environment.
3. At the Select Compatibility prompt, select your ESXi version.
   For more information on versions, see the Supported platforms.
4. When you are prompted to select a guest OS, set the following according to the Guest OS version that you are using:

Field	Setting
Guest OS Family	Linux
Guest OS Version	Oracle Linux 8 or 9 (64-bit)

5. Click **Next**.
6. On the Virtual Hardware tab of the Customize hardware page, make sure the VM configuration meets the following system resource recommendations:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

   Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:
   - More than four nodes in the Cryptographic Security Platform Vault cluster.
   - More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
   - More than 100,000 secrets stored.

   The rest of the options on this tab should be configured to match your vSphere environment.
   Note:
   - For the SCSI controller, we suggest that you use VMware Paravirtual. While other choices should work, VMware Paravirtual is used regularly in our testing.
   - For the network adapter type, we suggest that you use VMXNET 3. While other choices should work, VMXNET3 is used regularly in our testing.
7. On the VM Options tab of the Customize hardware page, expand Boot Options and set the Firmware to BIOS.
8. Connect the Cryptographic Security Platform Vault version 10.5.1 installation ISO image to the VM so that the VM will boot from this ISO image when you power on the VM. How you do this depends on how your vSphere environment is configured and what options you have available.
   For example, you could upload the Cryptographic Security Platform Vault ISO image to a datastore that vSphere can access and then attach the datastore ISO image as a CD/DVD drive that is connected when the VM powers on.
9. Power on the Cryptographic Security Platform Vault VM and have it boot from the Cryptographic Security Platform Vaultversion 10.5.1 installation ISO image .
10. When the VM boots from the ISO image, it will begin installing Oracle Linux.
    Note: The installer will post messages as the Oracle Linux operating system install proceeds. Some parts of the OS take longer to install than others, and there may be times when no new messages appear for over ten minutes. Do not attempt to cancel or restart the installation procedure during this time.
    The installer will automatically reboot the VM as needed.
    When then installer has finished, it displays a prompt asking for a password for the `htadmin` account.
11. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.

This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.

12. The System Configuration page asks if you want to use DHCP for the node. We highly recommend that you do *not* do this, as the Cryptographic Security Platform Vault node should always be available at a set IP address. Make sure **No** is selected and press **Enter** to acknowledge this message.
13. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.
14. On the System Configuration page, review the configuration settings and press **Enter** if you are ready to configure the node.
    The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
15. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
    When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
16. After the configuration is complete, power off your VM, detach the ISO, and reset the boot order. Then you can safely power on your VM again.
17. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
    a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
    b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
    Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
    c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
    d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
    e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
    f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
    g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
    If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
    To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
    h. When you are done, click **Continue**.
    i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
    Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.

j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI.

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Installing an Additional CSP Vault Cluster Node from an ISO Image.
- To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

Installing an Additional CSP Vault Cluster Node from an ISO Image

This procedure describes how to use the Entrust-provided ISO image to install and configure a new Cryptographic Security Platform Vault that you want to add to an existing cluster. If you want to configure a standalone Cryptographic Security Platform Vault node or the first node in the cluster, see Installing the First CSP Vault Node from an ISO Image.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Before You Begin

- If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.
- Make sure that the target VM can access the Entrust Cryptographic Security Platform Vault ISO image.
- Make sure the target VM meets the basic system requirements described in Requirements.
- If EMS is disabled, you will need to configure the node as a standalone node, disable EMS, and then join the cluster.
  For more information on EMS, see Configuring TLS. For more information on joining a cluster, see Joining a CSP Vault Cluster.

Note: If your version of vCenter is different from what is described below, please see your vCenter documentation for details about the ISO deployment process.

Procedure

1. Log into the vSphere Client.
2. Create a new virtual machine using the settings appropriate to your environment.
3. At the Select Compatibility prompt, select your ESXi version.
   For more information on versions, see the Supported platforms.
4. When you are prompted to select a guest OS, set the following according to the Guest OS version that you are using:

Field	Setting
Guest OS Family	Linux
Guest OS Version	Oracle Linux 8 or 9 (64-bit)

5. Click **Next**.
6. On the Virtual Hardware tab of the Customize hardware page, make sure the VM configuration meets the following system resource recommendations:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

The rest of the options on this tab should be configured to match your vSphere environment.

Note:

- For the SCSI controller, we suggest that you use VMware Paravirtual. While other choices should work, VMware Paravirtual is used regularly in our testing.
- For the network adapter type, we suggest that you use VMXNET 3. While other choices should work, VMXNET3 is used regularly in our testing.

7. On the VM Options tab of the Customize hardware page, expand Boot Options and set the Firmware to BIOS.
8. Connect the Cryptographic Security Platform Vault version 10.5.1 installation ISO image to the VM so that the VM will boot from this ISO image when you power on the VM. How you do this depends on how your vSphere environment is configured and what options you have available.
   For example, you could upload the Cryptographic Security Platform Vault ISO image to a datastore that vSphere can access and then attach the datastore ISO image as a CD/DVD drive that is connected when the VM powers on.
9. Power on the Cryptographic Security Platform Vault VM and have it boot from the Cryptographic Security Platform Vault version 10.5.1 installation ISO image .
10. When the VM boots from the ISO image, it will begin installing Oracle Linux.
    Note: The installer will post messages as the Oracle Linux operating system install proceeds. Some parts of the OS take longer to install than others, and there may be times when no new messages appear for over ten minutes. Do not attempt to cancel or restart the installation procedure during this time.
    The installer will automatically reboot the VM as needed.
    When then installer has finished, it displays a prompt asking for a password for the `htadmin` account.
11. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
    This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
    Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
12. The System Configuration page asks if you want to use DHCP for the node. We highly recommend that you do *not* do this, as the Cryptographic Security Platform Vault node should always be available at a set IP address. Make sure **No** is selected and press **Enter** to acknowledge this message.
13. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.

14. On the System Configuration page, review the configuration settings and press **Enter** if you are ready to configure the node.
    The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
15. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address).
    When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
16. After the configuration is complete, power off your VM, detach the ISO, and reset the boot order. Then you can safely power on your VM again.
17. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster using `secroot` for both the username and password.
18. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
    The Join Existing Cluster window displays.
19. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
    - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
    - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
    - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
    - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
20. Click **Continue**.
21. On the Download CSR page, click **Generate and Download CSR**.
22. Click **Continue**.
23. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
24. Select **Actions > Add a Node**.
25. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
26. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
27. Click **OK** to close the Add a Node window.
28. Return to the new node and click **Continue**.
29. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
30. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
31. When the node has successfully restarted, click **Login**.

What to Do Next

To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

CSP Vault ISO Installation for Bare Metal Server

ISO Installation Overview for Bare Metal Server

Entrust provides an ISO image that allows you to install the first Cryptographic Security Platform Vault node or add a Cryptographic Security Platform Vault node to an existing cluster.

To install CSP Vault on a bare metal server, see the following:

Prerequisites and Requirements for Installing CSP Vault on a Bare Metal Server

Before you begin the installation process, ensure that you meet the requirements in this section.

Hardware Prerequisites

Lenovo ThinkSystem SR250 or SR630 with:

- 8-core CPU
- 16 GB RAM
- Broadcom Ethernet Controller
- Intel VROC/VMD for NVMe RAID

Note: Only fresh installations are supported with this release.

Installation Requirements

- Configure RAID 1 so that 1 virtual disk is visible to the Operating System.
  When you deploy the ISO, the system will detect if the destination disk already has a formatted partition table. If so, you will be prompted to type 'delete my data' to proceed.
- Ensure that at least 1 NIC is connected. If you have multiple NICs, you will be prompted to select the primary interface.
- Ensure that UEFI is enabled.
- Ensure that UEFI secure boot is disabled. If not, you can disable it in XClarity Provisioning Manager by navigating to the UEFI Setup page and selecting **System Settings > Security > Secure Boot Configuration > Secure Boot Setting**.
  The deployment will not continue if UEFI Secure Boot is detected.
- If you plan to use network bonding, the primary bonded interface needs to be created with both members when you deploy the ISO. After the system setup is complete, you can create the secondary bonded interface.

Installing the First CSP Vault Node on a Bare Metal Server from an ISO

Note: Installing the ISO file will delete all existing data on the disk.

1. Mount the CSP Vault installation ISO in the media browser.
2. Make sure to change the one time boot option to CD/DVD by selecting F12 in the boot screen.
3. Start the installation.

4. When prompted, select the primary network interface for the installation.
5. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
6. If you want to configure a bonded interface, press **Yes** to enable bonding on the primary interface. Otherwise, press **No**.
   If you selected Yes, complete the following to configure the system with the bonded network interface:
   a. Choose the desired network bonding mode based on your network requirements, and press **OK**.
   b. Add the additional network interfaces that will participate in the bond and press **OK**.
   c. Enter any optional bonding parameters, such as link monitoring or failover settings, and press **OK**.
7. On the Confirm Network Configuration page, enter the appropriate network information for the CSP Vault node. When you are done, press **Enter** to save this information.
8. On the System Configuration page, review the configuration settings and press **Yes** if you are ready to configure the node.
   The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
9. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
10. After the configuration is complete, unmount the ISO from the media browser, and ensure that the boot order is reset.
11. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
    a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
    b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
       Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
    c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
    d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
    e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
    f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
    g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
       If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
       To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.

h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

12. If you would like to add an additional NIC or a bonded interface, you can configure it in the CSP Vault System Console by doing the following:
    a. From the System Console, navigate to Manage Network Settings and select Manage Interfaces and IP Address Settings.
    b. Choose one of the available unconfigured network interfaces and press **OK**.
    c. Select **Configure as secondary or bonded secondary interface** and press **OK**.
    d. Select **Yes** if you want to configure a bonded secondary interface, or select **No** if you want to configure an unbonded secondary interface.
    e. If you selected a bonded secondary interface, select the appropriate network bonding mode based on your network setup requirements and press **OK**.
    Note: If you selected unbonded, this step will not appear.
    f. If you selected a bonded secondary interface, add the additional interfaces that you want to be included in the secondary bond and press **OK**.
    Note: If you selected unbonded, this step will not appear.
    g. If you selected a bonded secondary interface, add any additional options for the bond, or leave blank if there are no additional options, and press **OK**.
    Note: If you selected unbonded, this step will not appear.
    h. When prompted to configure the selected interface, click **Yes**.
    i. Configure the secondary network and press **OK**.
    j. Verify that the secondary interface or network bond is successfully created and operational.

What to Do Next

- Connect the CSP Vault Appliance to CSP Compliance Manager.
- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Installing an Additional CSP Vault Node on a Bare Metal Server from an ISO.

Installing an Additional CSP Vault Node on a Bare Metal Server from an ISO

Note: Installing the ISO file will delete all existing data on the disk.

1. Mount the CSP Vault installation ISO in the media browser.
2. Make sure to change the one time boot option to CD/DVD by selecting F12 in the boot screen.
3. Start the installation.
4. When prompted, select the primary network interface for the installation.
5. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to

contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.

6. If you want to configure a bonded interface, press **Yes** to enable bonding on the primary interface. Otherwise, press **No**.
   If you selected Yes, complete the following to configure the system with the bonded network interface:
   a. Choose the desired network bonding mode based on your network requirements, and press **OK**.
   b. Add the additional network interfaces that will participate in the bond and press **OK**.
   c. Enter any optional bonding parameters, such as link monitoring or failover settings, and press **OK**.
7. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.
8. On the System Configuration page, review the configuration settings and press **Yes** if you are ready to configure the node.
   The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
9. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
10. After the configuration is complete, unmount the ISO from the media browser, and ensure that the boot order is reset.
11. Log into the webGUI on the CSP Vault node you want to join with the cluster using `secroot` for both the name and the password.
12. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
    The Join Existing Cluster window displays.
13. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
    - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
    - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
    - A passphrase to use during the joining process. Passphrase requirements are configured by a CSP Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
    - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
14. Click **Continue**.
15. On the Download CSR page, click **Generate and Download CSR**.
16. Click **Continue**.
17. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
18. Select **Actions > Add a Node**.
19. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
20. Click **OK** to close the Add a Node window.
21. Return to the new node and click **Continue**.
22. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.

23. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode. The node will restart after the join is complete.
24. When the node has successfully restarted, click **Login**.

CSP Vault in Amazon Web Services

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Amazon Web Services (AWS).

AWS Deployment Overview

To create a Cryptographic Security Platform Vault node in AWS, you need to launch a Entrust Cryptographic Security Platform Vault for AWS instance and then configure that instance using SSH.

After the first Cryptographic Security Platform Vault node is configured, you can then add additional nodes from other AWS availability zones or regions, or from other environments such as VMware vSphere or Microsoft Azure. All configuration information from the first node is copied to any subsequent nodes that you add to the cluster.

Note:

- CSP Vault now supports AWS Instance Metadata Service Version 2 (IMDSv2) to access EC2 instance metadata.
- CSP Vault does not support SSM manager. To access the console, use the EC2 console.

To create a Cryptographic Security Platform Vault cluster in AWS, perform the following tasks:

Step	Task	Details
1	Launch a Entrust Cryptographic Security Platform Vault for AWS instance that will become the initial Cryptographic Security Platform Vault node in the cluster.	Deploying the First CSP Vault Node in AWS.
2	Associate an Elastic IP (EIP) address with the instance.	Associating an Elastic IP Address with the CSP Vault Instance.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	Configuring the First CSP Vault Node in AWS.

Step	Task	Details
4	If desired, deploy additional Cryptographic Security Platform Vault nodes in AWS.	Deploying Additional CSP Vault Nodes in AWS.
5	Configure the additional nodes and join them to the existing cluster.	Configuring Additional CSP Vault Nodes in AWS.

Deploying the First CSP Vault Node in AWS

In order to deploy the first Cryptographic Security Platform Vault node on AWS, you need to launch a Entrust Cryptographic Security Platform Vault for AWS instance on a new or existing VPC. After you have configured the first Cryptographic Security Platform Vault node, you can add other Cryptographic Security Platform Vault nodes to your Cryptographic Security Platform Vault cluster as desired.

Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

1. Open a web browser and navigate to the Amazon Web Services login page for your company. The default login page is https://aws.amazon.com/.
2. Log in to the AWS Management Console with your AWS user name and password.
3. In the top menu bar just after your login name, verify that the deployment region is correct. If you need to change it, click the current region and select the new region from the drop-down list.
4. Create a new VPC to use for the Cryptographic Security Platform Vault node, or select an existing VPC.
5. In the top menu bar, select **Services > Compute > EC2**.
6. Click the blue **Launch Instance** button.
7. In the Step 1: Choose an Amazon Machine Image (AMI) page, click **AWS Marketplace** in the left-hand pane.
8. Search the Marketplace for "Entrust" and select Entrust Cryptographic Security Platform Vault **for AWS BYOL** (Bring Your Own License).
9. Review the details and click **Continue**.
10. In the Step 2: Choose an Instance Type page, select an instance type. For optimal performance, we recommend that you select a general purpose or compute optimized instance type with SSD Instanced storage, such as **m3.large** or **c3.large**. The Cryptographic Security Platform Vault system resource recommendations are:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.

- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

11. After you have selected the type, click **Next: Configure Instance**
12. On the Step 3: Configure Instance Details page, set the following options:
    - Number of Instances —Specify the number of instances you want to launch in this field. All instances will run in the same region using the same VPC and instance settings.
      Tip: You can use this option to create a multi-node Cryptographic Security Platform Vault cluster on this VPC without needing to launch additional instances, but you can also add additional Cryptographic Security Platform Vault nodes to the cluster at any time after the initial node has been configured.
    - Network —Select the VPC you want to use for the Cryptographic Security Platform Vault node.
    - Set all other options on this page according to your corporate standards.
13. When you are done, click **Next: Add Storage**.
14. On the Step 4: Add Storage page, set the following options:
    - Volume Size —Set the size of the disk based on your configuration requirements. The default setting of65 GB should work for most Cryptographic Security Platform Vault installations.
    - Volume Type—For optimal performance, we recommend setting the volume type to one of the SSD options instead of the default Magnetic volume.
    - Delete on Termination—If you select this option and the instance is deleted, all keys stored on this Cryptographic Security Platform Vault node will be deleted as well. In a single node configuration, this means that encrypted data cannot be decrypted, as the keys will be lost. If you want to use this option, make sure all data is decrypted before the instance is deleted.
15. When you are done, click **Next: Add Tags**.
16. On the Step 5: Add Tags page, click **Add Tag** and enter a Name tag for the instance:
    - Key —Enter "Name".
    - Value—Enter the name for this Cryptographic Security Platform Vault node.

    Add any other tags as desired.
17. When you are done, click **Next: Configure Security Group**.
18. In the Step 6: Configure Security Group page, do the following:
    a. Make sure that the **Assign a security group** field is set to **Create a new security group**.
       Note: You can use an existing security group as long as all of the required ports are open in that security group.
    b. Optionally enter a custom security group name and description in the **Security group name** and **Description** fields.
    c. For each of the required entries in the security group, set the Source IP addresses or security groups that can communicate with Cryptographic Security Platform Vault through the associated ports. We strongly recommend that you do *not* use the default 0.0.0.0/0 notation, which indicates that the ports are open to the world.

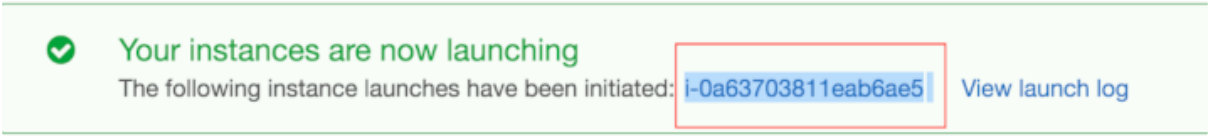
Cryptographic Security Platform Vault requires the following ports:

Type	Protocol	Port Range	Source
SSH (22)	TCP	22	*IP address list or another security group*
HTTPS (443)	TCP	443	*IP address list or another security group*
Custom TCP Rule	TCP	5432	*IP address list or another security group*
Custom TCP Rule	TCP	8443	*IP address list or another security group*

Type	Protocol	Port Range	Source
Custom UDP Rule	UDP	123	*IP address list or another security group*

For details about specifying the source IP addresses or security groups, see your AWS documentation.

19. When you are done, click **Review and Launch**.
20. In the Step 7: Review Instance Launch page, verify your selections and click **Launch**.
21. At the prompt, either select an existing key pair or select **Create a new key pair**, specify a key pair name, and download the new private key file for the new key pair.
22. When you are done, click **Launch Instances**. AWS displays a confirmation page stating that your instance is being launched and displays the instance ID. Make a note of the ID, as it will be your initial Cryptographic Security Platform Vault password.



To verify the status of the instance, select **Services > EC2 > Instances** and locate the new instance in the table.

Tip: If you requested multiple instances on the Step 3: Configure Instance Details page, you will see multiple Cryptographic Security Platform Vault instances with the same name listed in the table. We recommend that you give each instance a unique name at this point so that you can tell them apart as you configure them. To do so, mouse over an instance name and click the pencil icon when it appears.

What to Do Next

Associate an Elastic IP address with the instance as described in Associating an Elastic IP Address with the CSP Vault Instance. An elastic IP address is required for every Cryptographic Security Platform Vault instance so that you can configure and maintain the Cryptographic Security Platform Vault instance using a static IPv4 address.

If you created multiple instances, you need to assign a different Elastic IP to each copy of the instance.

Associating an Elastic IP Address with the CSP Vault Instance

An elastic IP address is a static IPv4 address that allows you to access the Cryptographic Security Platform Vault AWS instance from a web browser. An elastic IP address is required in order to configure and maintain the Cryptographic Security Platform Vault node using the Cryptographic Security Platform Vault webGUI and the Entrust Cryptographic Security Platform Vault System Console.

> Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

1. In the Amazon Management Console's top menu bar, select **Services > EC2**.
2. In the EC2 Dashboard, select **Network & Security > Elastic IPs**.
3. Click the blue **Allocate new address** button.
4. Click **Allocate**.
5. Make a note of the new IP address and click **Close**.
6. In the table of elastic IP addresses, select the EIP address you just created.
7. Select **Actions > Associate address**.
8. On the Associate Address page, select the Cryptographic Security Platform Vault instance in the **Instance** drop-down list, then click **Associate**.
9. On the confirmation page, click **Close**.

10. Repeat this procedure for any other Cryptographic Security Platform Vault instance that does not have an associated IPv4 Public IP address.
11. When you have assigned all Cryptographic Security Platform Vault instances an EIP address, from the EC2 Dashboard, select **Instances**.
12. In the table, locate your Cryptographic Security Platform Vault instances and make sure the correct elastic IP addresses appear in the **IPv4 Public IP** column.

What to Do Next

If this is the first Cryptographic Security Platform Vault node in the cluster, configure it as described in Configuring the First CSP Vault Node in AWS.

If you are adding this node to an existing Cryptographic Security Platform Vault cluster, see Configuring Additional CSP Vault Nodes in AWS.

Configuring the First CSP Vault Node in AWS

You need to configure the Cryptographic Security Platform Vault instance using SSH before you can use the Cryptographic Security Platform Vault webGUI to configure and maintain your Cryptographic Security Platform Vault cluster.

The following procedure describes how to configure the first Cryptographic Security Platform Vault node in the cluster. If you are adding this node to an existing cluster, see Configuring Additional CSP Vault Nodes in AWS.

Before You Begin

Make sure you have the following information:

- The Amazon instance ID for the Cryptographic Security Platform Vault instance.
- The Elastic (Public) IP address associated with the instance.
- The private key file (in pem format) that was used when the instance was created.

Tip: To find this information, select Instances from the Amazon Management Console EC2 Dashboard, then select the Cryptographic Security Platform Vault instance in the table. In the Description tab, look at the Instance ID, IPv4 Public IP, and Key pair name fields.

Procedure

1. To initialize Cryptographic Security Platform Vault for this cluster, do the following:
    a. Use a web browser to navigate to `https://<Elastic-IP-addy>`, where `<Elastic-IP-addy>` is the Elastic IP address associated with the Cryptographic Security Platform Vault AWS instance. For security reasons, you must explicitly specify `https://` in the URL.
    b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
    Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
    c. On the **Entrust Cryptographic Security Platform Vault Management** login, enter `secroot` for the username and the AWS instance ID as the password.
    d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
    e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
    f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.

g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

2. Optional. Log into the `htadmin` account on the keycontrol System Console using the private key file. For example:
`ssh -i <key-file>.pem htadmin@<Elastic-IP-addy>`
The password is the same as the secroot password that you changed in step **f** above.
Important: The secroot password is used for this first login. You can either change it, or leave it as is. If you change the `htadmin` password in the System Console, it only changes the password for this particular node, and does not affect the secroot password.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Deploying Additional CSP Vault Nodes in AWS.
- For information about configuring and maintaining your Cryptographic Security Platform Vault cluster, see the CSP Vault Cluster Maintenance.

Deploying Additional CSP Vault Nodes in AWS

The following procedure describes how to deploy a Cryptographic Security Platform Vault node that you intend to add to an existing Cryptographic Security Platform Vault cluster. If you want to deploy a Cryptographic Security Platform Vault node that will become the first node in a new cluster, see Configuring the First CSP Vault Node in AWS.

> Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

Before You Begin

If you want to use a existing VPC for the new node that is different from the VPC used for the first Cryptographic Security Platform Vault node, make sure that you have set up VPC-to-VPC communication between the VPCs. This includes configuring a Peering Connection and setting the correct Routing Table information. For details, see your AWS documentation.

If you want to use the same VPC for the new node as you used for the first node, make sure you know the following information:

- The region in which the first node is deployed.
- The VPC assigned to the first node.
- The Security Group assigned to the first node.

Tip: To find this information, select Instances from the Amazon Management Console EC2 Dashboard, then select the first Cryptographic Security Platform Vault node in the table. In the Description tab, look at the VPC ID and Security groups fields.

Procedure

1. Open a web browser and navigate to the Amazon Web Services login page for your company. The default login page is https://aws.amazon.com/.
2. Log in to the AWS Management Console with your AWS user name and password.
3. In the top menu bar just after your login name, select the Region into which you want to deploy the Cryptographic Security Platform Vault node. If you want to use the same VPC as the first Cryptographic Security Platform Vault node, you must deploy the new node in the same region as the first node.
4. If you intend to use the same VPC as you used for the first Cryptographic Security Platform Vault node, proceed to the next step. Otherwise, make sure that you have configured VPC-to-VPC communication between the two VPCs as per your AWS documentation.
5. In the top menu bar, select **Services > Compute > EC2**.
6. Click the blue **Launch Instance** button.
7. In the Step 1: Choose an Amazon Machine Image (AMI) page, click **AWS Marketplace** in the left-hand pane.
8. Search the Marketplace for "Entrust" and select Entrust Cryptographic Security Platform Vault **for AWS BYOL** (Bring Your Own License).
9. Review the details of the version you selected and click **Continue**.
10. In the Step 2: Choose an Instance Type page, select an instance type. For optimal performance, we recommend that you select a general purpose or compute optimized instance type with SSD Instanced storage, such as **m3.large** or **c3.large**. The Cryptographic Security Platform Vault system resource recommendations are:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

11. After you have selected the type, click **Next: Configure Instance Details**.
12. On the Step 3: Configure Instance Details page, set the following options:
    - Number of Instances—Specify the number of instances you want to launch in this field. All instances will run in the same region using the same VPC and instance settings.
    - Network —Select the VPC you want to use for the Cryptographic Security Platform Vault node.
    - Set all other options on this page according to your corporate standards.
13. When you are done, click **Next: Add Storage**.
14. On the Step 4: Add Storage page, set the following options:
    - Volume Size —Set the size of the disk based on your configuration requirements. The default setting of 20 GB should work for most Cryptographic Security Platform Vault installations.

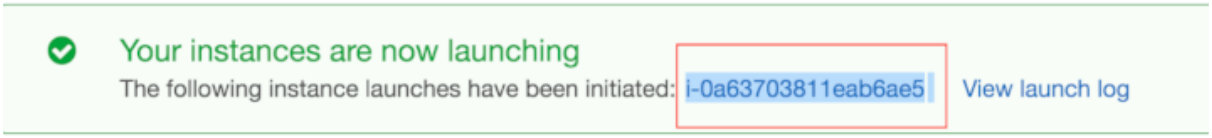
- Volume Type—For optimal performance, we recommend setting the volume type to one of the SSD options instead of the defaut Magnetic volume.
- Delete on Termination—If you select this option and the instance is deleted, all keys stored on this Cryptographic Security Platform Vault node will be deleted as well. In a single node configuration, this means that encrypted data cannot be decrypted, as the keys will be lost. If you want to use this option, make sure all data is decrypted before the instance is deleted.

15. When you are done, click **Next: Add Tags**.
16. On the Step 5: Add Tags page, click **Add Tag** and enter a Name tag for the instance:
    - Key —Enter "Name".
    - Value—Enter the name for this Cryptographic Security Platform Vault node.

    Add any other tags as desired.
17. When you are done, click **Next: Configure Security Group**.
18. In the Step 6: Configure Security Group page **Assign a security group** field, do one of the following:
    - Select **Select an existing security group** and then select the security group you assigned to the first Cryptographic Security Platform Vault node.
      Note: You can use any existing security group as long as all of the required ports are open in that security group.
    - Select **Create a new security group**. For each of the required entries in the security group, set the Source IP addresses or security groups that can communicate with Cryptographic Security Platform Vault through the associated ports. We strongly recommend that you do *not* use the default 0.0.0.0/0 notation, which indicates that the ports are open to the world.
      Cryptographic Security Platform Vault requires the following ports:

Type	Protocol	Port Range	Source
SSH (22)	TCP	22	*IP address list or another security group*
HTTPS (443)	TCP	443	*IP address list or another security group*
Custom TCP Rule	TCP	5432	*IP address list or another security group*
Custom TCP Rule	TCP	8443	*IP address list or another security group*
Custom UDP Rule	UDP	123	*IP address list or another security group*

      For details about specifying the source IP addresses or security groups, see your AWS documentation.
19. When you are done, click **Review and Launch**.
20. In the Step 7: Review Instance Launch page, verify your selections and click **Launch**.
21. At the prompt, either select an existing key pair or select **Create a new key pair**, specify a key pair name, and download the new private key file for the new key pair.
22. When you are done, click **Launch Instances**. AWS displays a confirmation page stating that your instance is being launched and displays the instance ID. Make a note of the ID, as it will be your initial Cryptographic Security Platform Vault password.



23. To verify the status of the instance, select **Services > EC2 > Instances** and locate the new instance in the table.
    Tip: If you requested multiple instances on the Step 3: Configure Instance Details page, you will see multiple Cryptographic Security Platform Vault instances with the same name listed in the table. We recommend that you give each instance a unique name at this point so that you can tell them apart as you configure them. To do so, mouse over an instance name and click the pencil icon when it appears.

What to Do Next

Associate an Elastic IP address with the instance as described in Associating an Elastic IP Address with the CSP Vault Instance. An elastic IP address is required for every Cryptographic Security Platform Vault instance so that you can configure and maintain the Cryptographic Security Platform Vault instance using a static IPv4 address.

If you created multiple instances, you need to assign a different Elastic IP to each copy of the instance.

Configuring Additional CSP Vault Nodes in AWS

After the AWS instance is deployed, you need to configure the Cryptographic Security Platform Vault node using SSH. The following procedure describes how to configure the node as part of an existing Cryptographic Security Platform Vault cluster. If you want to configure this node as the first node in the Cryptographic Security Platform Vault cluster, see Configuring the First CSP Vault Node in AWS.

Before You Begin

Make sure that the new Cryptographic Security Platform Vault node can communicate with the Cryptographic Security Platform Vault nodes in the existing Cryptographic Security Platform Vault cluster. For details, see your AWS documentation.

Make sure you have the following information:

- The Amazon instance ID for the new Cryptographic Security Platform Vault instance.
- The Elastic (Public) IP address associated with the new instance.
- The private key file (in pem format) that was used when the new instance was created.
  Tip: To find this information, select **Instances** from the Amazon Management Console EC2 Dashboard, then select the Cryptographic Security Platform Vault instance in the table. In the **Description** tab, look at the **Instance ID**, **IPv4 Public IP**, and **Key pair name** fields.
- The private IP address of one of the existing Cryptographic Security Platform Vault nodes in the cluster.
  Tip: To find this IP address, log into the Cryptographic Security Platform Vault webGUI on one of the existing nodes and click **Cluster** in the top menu bar. Go to the **Servers** tab and look at the IP address in the table.

Procedure

1. Use a web browser to navigate to `https://<Elastic-IP-addy>`, where `<Elastic-IP-addy>` is the Elastic IP address associated with the Cryptographic Security Platform Vault AWS instance. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Login** page, enter `secroot` for the username and the AWS instance ID as the password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.

6. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
    - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
    - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
    - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
    - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.
19. Optional. Log into the `htadmin` account on the keycontrol System Console using the private key file. For example:
    `ssh -i <key-file>.pem htadmin@<Elastic-IP-addy>`
    The password is the Amazon instance ID.
    After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

CSP Vault in Google Cloud Platform

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Google Cloud Platform (GCP).

- Configuring Additional GCP Nodes

GCP Deployment Overview

To create a Cryptographic Security Platform Vault cluster in GCP, perform the following tasks:

Step	Task	Details
1	Launch an Entrust Cryptographic Security Platform Vault for GCP instance that will become the initial Cryptographic Security Platform Vault node in the cluster.	Deploying the First CSP Vault Node in GCP.
2	Configure firewall rules for the Cryptographic Security Platform Vault instance.	Configuring Firewall Rules for the CSP Vault Instance.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	Configuring the First GCP Node.
4	If desired, deploy additional Cryptographic Security Platform Vault nodes in GCP using the same instructions as the first node.	Deploying the First CSP Vault Node in GCP.
5	Configure the additional nodes and join them to the existing cluster.	Configuring Additional GCP Nodes.

Deploying the First CSP Vault Node in GCP

In order to deploy the first Cryptographic Security Platform Vault node on GCP, you need to launch Entrust Cryptographic Security Platform Vault for GCP from the Google Cloud Marketplace.

1. Log in to the GCP Console.
2. Select your project.
3. Search for the **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL** image in the Google Cloud Marketplace.
4. Click **Launch**.
5. On the New deployment page, enter the Deployment name, the Service Account information, and the Zone. For Machine type, we recommend using n1-standard-2 (2 vCPU, 1 core, 7.5 GB memory).
6. In the firewall section, ensure that you select **Allow HTTPS traffic from the Internet**.
   Note: You will need to enter additional firewall rules. For details, see Configuring Firewall Rules for the CSP Vault Instance.
7. Click **Deploy**.
8. After the instance is created, locate your new VM on the **Compute Engine > VM Instances** page and copy the External IP address.

Configuring Firewall Rules for the CSP Vault Instance

Before configuring Cryptographic Security Platform Vault, ensure that the following ports are open in your GCP firewall.

Type	Protocol	Port Range
SSH (22)	TCP	22
HTTPS (443)	TCP	443
Custom TCP Rule	TCP	8443
Custom TCP Rule	TCP	5432
Custom UDP Rule	UDP	123

If you are going to use Cryptographic Security Platform Vault as a KMIP server or want to use the SNMP polling feature for Cryptographic Security Platform Vault, you must open related ports for the Cryptographic Security Platform Vault instance.

Type	Protocol	Default Port
KMIP	TCP	5696
SNMP	UDP	161

Note: These feature specific ports are configurable, and you must ensure you configure the firewall rules accordingly.

To set up the firewall, select VPC network > Firewall in the GCP Console. The Dashboard shows you a set of firewall rules. Select the Create Firewall Rules button to configure additional firewall rules.

Configuring the First GCP Node

Follow this procedure if you are configuring the first Cryptographic Security Platform Vault node in the cluster. If you are adding the node to an existing cluster, see Configuring Additional GCP Nodes.

Before You Begin

Make sure you have the following information:

- The instance ID for the Cryptographic Security Platform Vault instance. This is located in the Basic Information section on the Details page of the instance.
- The External IP associated with the instance.

Procedure

To initialize Cryptographic Security Platform Vault for this cluster, do the following:

1. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the External IP address. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and the Instance ID for the password.
4. Click **Login**.
5. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
6. On the Welcome to Appliance Management screen, click **Continue as a Standalone Node**.
7. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
8. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
   If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
   To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
9. When you are done, click **Continue**.
10. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
    Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
11. When you are finished, click **Continue**.
    Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the Administration Guide.

What to Do Next

If you want to add another Cryptographic Security Platform Vault node to this cluster, create another instance as described in Deploying the First CSP Vault Node in GCP and then configure it as described in Configuring Additional GCP Nodes.

Configuring Additional GCP Nodes

If you deploy an additional Cryptographic Security Platform Vault on GCP, you can add it to your existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Ensure that the new Cryptographic Security Platform Vault node can communicate with the nodes in the existing Cryptographic Security Platform Vault cluster.
- Ensure that you have the following information:
  - The instance ID for the new Cryptographic Security Platform Vault instance. This is located in the Basic Information section on the Details page of the instance.
  - The External IP associated with the new instance.
  - The private IP address of one of the existing Cryptographic Security Platform Vault nodes in the cluster.
    Tip: To find this IP address, log into the Cryptographic Security Platform Vault webGUI and click Switch to Appliance Management. Click Clusters in the top menu bar, then navigate to the Servers tab to see the IP address.

Procedure

1. Use a web browser to navigate to `https://<Public-IP-addy>`, where `<Public-IP-addy>` is the Public IP address assigned to the Cryptographic Security Platform Vault VM. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and the Instance ID for the password.
4. Click **Login**.
5. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
6. On the Welcome to Appliance Management screen, click **Join an Existing Cluster.**.
   The Join Existing Cluster window displays.
7. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so that you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
8. Click **Continue**.
9. On the Download CSR page, click **Generate and Download CSR**.
10. Click **Continue**.
11. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
12. Select **Actions > Add a Node**.
13. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
14. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
15. Click **OK** to close the Add a Node window.
16. Return to the new node and click **Continue**.
17. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address of any node in the existing cluster, and enter the passphrase that you selected.
18. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
19. When the node has successfully restarted, click **Login**.
20. Optional. Log into the `htadmin` account on the Cryptographic Security Platform VaultSystem Console using the private key file. For example:

`ssh -i <key-file>.pem htadmin@<Public-IP-addy>`

The password is the VM unique ID (vmId).

After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

CSP Vault in Microsoft Azure

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Microsoft Azure.

Azure Deployment Overview

In order to deploy a Cryptographic Security Platform Vault node in a Microsoft Azure environment, you need to:

1. Deploy a Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl) virtual machine (VM) resource from the Azure Marketplace. For details, see Deploying a CSP Vault Node in Azure.
2. Use SSH to configure the new Cryptographic Security Platform Vault node. How you do this depends on whether this is the first Cryptographic Security Platform Vault node in the cluster or if you are adding this node to an existing Cryptographic Security Platform Vault cluster.
    - If this is the first node in the cluster, configure the node and initialize the Cryptographic Security Platform Vault webGUI. For details, see Configuring the First CSP Vault Node in Azure.
    - If you are adding this node to an existing Cryptographic Security Platform Vault cluster, configure the node and authenticate it with the existing cluster. For details, see Configuring Additional CSP Vault Nodes in Azure.

Recommendations

When working with Microsoft Azure, Entrust recommends the following:

- If your corporate Azure subscription is shared among multiple users, we recommend you use the Azure Resource Manager to lock the Cryptographic Security Platform Vault resources in the resource group so that they are not accidentally deleted.
- If you deploy multiple Cryptographic Security Platform Vault nodes in Azure to create your Cryptographic Security Platform Vault cluster, we recommend that the nodes be in different regions and resource groups to provide high availability.
- If you need to move a Cryptographic Security Platform Vault node to another region, we recommend that you deploy a new Cryptographic Security Platform Vault node in the new region, add that node to the existing cluster, and then delete the old Cryptographic Security Platform Vault node.

Deploying a CSP Vault Node in Azure

To deploy a Cryptographic Security Platform Vault node in Microsoft Azure, you need to create a virtual machine (VM) resource that has a Public IP address and SSH access. After Azure has started the new VM, you can configure it to either become the first node in a Cryptographic Security Platform Vault cluster or you can join the new node with an existing cluster.

The following procedure describes how to create the VM resource. Configuration details, see Configuring Additional CSP Vault Nodes in Azure.

> Note: If your version of ARM is different from what is described below, please see your Azure documentation.

Before You Begin

Make sure you have access to a public SSH key pair that you can use for this instance. You will be required to paste the public portion of the key pair into the Create Virtual Machine wizard and you will need the private portion of the key pair when you configure the new VM.

Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.

Procedure

1. Log into your Microsoft Azure account.
2. In the left-hand pane, click **Create a resource**.
3. In the Search bar, enter "Entrust".
4. Select **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl)**.
5. Review the information and then click **Create** at the bottom of the right-hand pane.
6. On the **Basics** page, specify the options you want to use:

Field	Description
Project Details Section	
Subscription	Select the Azure subscription that you want to use.
Resource group	If this is the first Cryptographic Security Platform Vault node you are deploying, you can create a new resource group or use an existing group as desired. If you want to connect this Cryptographic Security Platform Vault node with an existing node, make sure you select the same resource group as the existing Cryptographic Security Platform Vault node.
Instance Details	
Virtual machine name	The name of the VM that will host the Cryptographic Security Platform Vault node.
Region	Select the region in which this Cryptographic Security Platform Vault node should be deployed. If you want to connect this node to an existing Azure Cryptographic Security Platform Vault node, select the same region as the existing node or make sure a communication channel exists between the two regions.
Availability options	Select the desired availability option. Cryptographic Security Platform Vault does *not* require any special infrastructure redundancy.

Field	Description
Image	Make sure this is set to Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl).
Size	Select the size of the VM that you want to use for Cryptographic Security Platform Vault. Entrust recommends the following for standard and large deployments: • VCPUs: 2 for standard, 4 for large. • RAM: 8 GB for standard, 16 GB for large.
Administrator Account	
Authentication type	Select SSH public key.
Username	Enter `htadmin` as the username. The username must be in lower case.
SSH public key	Paste in the public portion of the SSH key pair you want to use for this node.

7. When you are done, click **Next: Disks**.
8. On the **Disks** tab, specify the options you want to use. For optimum performance, we recommend you select an SSD disk type. Cryptographic Security Platform Vault does not require additional data disks.
9. When you are done, click **Next: Networking**.
10. On the **Networking** page, specify the options you want to use based on your corporate standards. Cryptographic Security Platform Vault only requires the following:
    - The Public IP address must be static, which it is *not* by default. To use a static IP address, click **Create New** under the **Public IP** field. On the **Create public IP address** page, enter a name for the IP address and select the **Static** radio button under **Assignment**. When you are done, click **OK**.
    - If you create a new Network Security Group in this step (which is the Azure default action), Cryptographic Security Platform Vault automatically creates the correct port settings. If you select an existing Network Security Group, you need to make sure the security group allows network communication with Cryptographic Security Platform Vault over the following ports and protocols:

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443
Custom	TCP	5432
Custom	TCP	8443
Custom	UDP	123

If you plan to connect this node with an existing Cryptographic Security Platform Vault cluster, you may need to open additional ports if the nodes are running in different Azure regions or in different environments.

11. If you want to set any other options for the VM, do so. When you are done, click **Review + Create**.
12. Review the settings for the resource and click **Create**. Wait for the success message from Azure confirming that the new resource is running and ready to use.
13. After Azure has created the virtual machine, determine the public IP address. To do so:
    a. In the left-hand pane, select **Resource groups**.
    b. Click the name of the resource group you specified on the **Basics** page.
    c. Click the virtual machine name in the table.
    Tip: If you do this before Azure has deployed the new VM, it may take a few minutes for the VM name to appear in this table.
    Azure displays the public IP address in the **Public IP address** field in the VM Details area.
14. Configure the node as the first Cryptographic Security Platform Vault node in the cluster or add it to an existing Cryptographic Security Platform Vault cluster. For details, see:
    - Configuring the First CSP Vault Node in Azure
    - Configuring Additional CSP Vault Nodes in Azure

Configuring the First CSP Vault Node in Azure

To deploy a Cryptographic Security Platform Vault node in Microsoft Azure, you need to create a virtual machine (VM) resource that has a Public IP address and SSH access. After Azure has started the new VM, you can configure it to either become the first node in a Cryptographic Security Platform Vault cluster or you can join the new node with an existing cluster.

The following procedure describes how to create the VM resource. Configuration details, see Configuring Additional CSP Vault Nodes in Azure.

> Note: If your version of ARM is different from what is described below, please see your Azure documentation.

Before You Begin

Make sure you have access to a public SSH key pair that you can use for this instance. You will be required to paste the public portion of the key pair into the Create Virtual Machine wizard and you will need the private portion of the key pair when you configure the new VM.

Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.

Procedure

1. Log into your Microsoft Azure account.
2. In the left-hand pane, click **Create a resource**.
3. In the Search bar, enter "Entrust".
4. Select **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl)**.
5. Review the information and then click **Create** at the bottom of the right-hand pane.
6. On the **Basics** page, specify the options you want to use:

Field	Description
Project Details Section	
Subscription	Select the Azure subscription that you want to use.

Field	Description
Resource group	If this is the first Cryptographic Security Platform Vault node you are deploying, you can create a new resource group or use an existing group as desired. If you want to connect this Cryptographic Security Platform Vault node with an existing node, make sure you select the same resource group as the existing Cryptographic Security Platform Vault node.
Instance Details	
Virtual machine name	The name of the VM that will host the Cryptographic Security Platform Vault node.
Region	Select the region in which this Cryptographic Security Platform Vault node should be deployed. If you want to connect this node to an existing Azure Cryptographic Security Platform Vault node, select the same region as the existing node or make sure a communication channel exists between the two regions.
Availability options	Select the desired availability option. Cryptographic Security Platform Vault does *not* require any special infrastructure redundancy.
Image	Make sure this is set to Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl).
Size	Select the size of the VM that you want to use for Cryptographic Security Platform Vault. Entrust recommends the following for standard and large deployments: • VCPUs: 2 for standard, 4 for large. • RAM: 8 GB for standard, 16 GB for large.
Administrator Account	
Authentication type	Select SSH public key.
Username	Enter `htadmin` as the username. The username must be in lower case.
SSH public key	Paste in the public portion of the SSH key pair you want to use for this node.

7. When you are done, click **Next: Disks**.
8. On the **Disks** tab, specify the options you want to use. For optimum performance, we recommend you select an SSD disk type. Cryptographic Security Platform Vault does not require additional data disks.

9. When you are done, click **Next: Networking**.
10. On the **Networking** page, specify the options you want to use based on your corporate standards. Cryptographic Security Platform Vault only requires the following:
    - The Public IP address must be static, which it is *not* by default. To use a static IP address, click **Create New** under the **Public IP** field. On the **Create public IP address** page, enter a name for the IP address and select the **Static** radio button under **Assignment**. When you are done, click **OK**.
    - If you create a new Network Security Group in this step (which is the Azure default action), Cryptographic Security Platform Vault automatically creates the correct port settings. If you select an existing Network Security Group, you need to make sure the security group allows network communication with Cryptographic Security Platform Vault over the following ports and protocols:

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443
Custom	TCP	5432
Custom	TCP	8443
Custom	UDP	123

    If you plan to connect this node with an existing Cryptographic Security Platform Vault cluster, you may need to open additional ports if the nodes are running in different Azure regions or in different environments.
11. If you want to set any other options for the VM, do so. When you are done, click **Review + Create**.
12. Review the settings for the resource and click **Create**. Wait for the success message from Azure confirming that the new resource is running and ready to use.
13. After Azure has created the virtual machine, determine the public IP address. To do so:
    a. In the left-hand pane, select **Resource groups**.
    b. Click the name of the resource group you specified on the **Basics** page.
    c. Click the virtual machine name in the table.
    Tip: If you do this before Azure has deployed the new VM, it may take a few minutes for the VM name to appear in this table.

    Azure displays the public IP address in the **Public IP address** field in the VM Details area.
14. Configure the node as the first Cryptographic Security Platform Vault node in the cluster or add it to an existing Cryptographic Security Platform Vault cluster. For details, see:
    - Configuring the First CSP Vault Node in Azure
    - Configuring Additional CSP Vault Nodes in Azure

Configuring Additional CSP Vault Nodes in Azure

You can add a Cryptographic Security Platform Vault node running in the Azure environment to any other Cryptographic Security Platform Vault nodes running in any other environments as long as the Azure node can communicate with the other nodes in the cluster.

Before You Begin

- Make sure you have the private SSH key file that matches the public SSH key that was specified when the instance was created.

Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.

- Make sure you know the static public IP address associated with the Azure node.
  To find the public IP address, select **All resources** from the Azure Resource Manager dashboard, then click on the virtual machine name on which the Cryptographic Security Platform Vault node is running. The public IP address is displayed in the VM details section at the top of the page.
- Make sure you know the IP address of one of the Cryptographic Security Platform Vault nodes already in the cluster.
  This IP address may *not* be the same as the public IP address. Make sure you verify the IP address before you attempt to add the node to the cluster.
  To find the correct IP address, log into the Cryptographic Security Platform Vault webGUI with Domain Admin privileges and go to **Cluster > Servers**. The IP address for each Cryptographic Security Platform Vault node is listed in the table.
- Make sure that the Azure node can communicate with the Cryptographic Security Platform Vault cluster in which you want to add the node. For details on setting up communication between the Azure VM and a Cryptographic Security Platform Vault VM running in a different Azure location or a different environment such as vSphere or AWS, see your Azure documentation.

Important: Azure might disconnect ssh sessions if idle for more than 5 minutes. To prevent this, please use the ServerAliveInterval and ServerAliveCountMax opens in the ssh client command line to keep the session active during Cryptographic Security Platform Vault management.

We recommend using ssh CLI options to send a KeepAlive packet with a frequency duration of less than 5 minutes. Please refer to the sshd_config man page for how to use the ServerAliveInterval and ServerAliveCountMax options. For example:

```
ssh -o ServerAliveInterval=180 -o ServerAliveCountMax=10 user@host
```

Procedure

1. Use a web browser to navigate to `https://<Public-IP-addy>`, where `<Public-IP-addy>` is the Public IP address Azure assigned to the Cryptographic Security Platform Vault VM. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and enter the VM unique ID (vmId) for the password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
6. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.

- Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.

7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.
19. Optional. Log into the `htadmin` account on the Cryptographic Security Platform Vault System Console using the private key file. For example:
    `ssh -i <key-file>.pem htadmin@<Public-IP-addy>`
    The password is the VM unique ID (vmId).
    After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

7 Initializing the CSP Vault Management webGUI

The first time you log into the Cryptographic Security Platform Vault Management webGUI for a Cryptographic Security Platform Vault node, you need to do some basic initialization. After this process is complete, you can log directly into the Cryptographic Security Platform Vault Management webGUI without going through these steps.

1. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address you specified during installation. For security reasons, you must explicitly specify `https://` in the URL.
   Tip: If you do not know the Management IP address for the node, log into the system on which the node is installed as `htadmin`. Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. From the menu, select **Manage Network Settings > Show Current Network Configuration**.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
6. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
7. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
   If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
   To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
8. When you are done, click **Continue**.
9. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
   Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
10. When you are finished, click **Continue**.
    Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see CSP Vault Management webGUI Page Reference.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster:
  - For OVA, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install).
  - For ISO, see CSP Vault ISO Installation for Hypervisor.
- If you plan to use the Entrust Policy Agent on either the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption, see Preparing to Install the Policy Agent.

.

8 Upgrading CSP Vault

CSP Vault Upgrade Paths

Important: Beginning with version 10.4.7, you will no longer be allowed to upgrade if your license is not current. If you see an error message, please contact support at https://trustedcare.entrust.com.

If your Cryptographic Security Platform Vault nodes are running version 10.4.3 or later, you can upgrade the entire cluster from any node in the cluster using the Cryptographic Security Platform Vault Management webGUI. Cryptographic Security Platform Vault automatically applies the upgrade to all nodes in the cluster sequentially so that the Cryptographic Security Platform Vault cluster remains available for key requests from the registered VMs throughout the entire upgrade process.

You can only upgrade between successive versions. Supported upgrade paths are:

Initial Release	Available Upgrade Paths
10.5.1	10.6.1
10.4.7	10.5.1, 10.6.1
10.4.5	10.4.7, 10.5.1, 10.6.1
10.4.3	10.4.5, 10.4.7, 10.5.1, 10.6.1

Important: You must upgrade the Cryptographic Security Platform Compliance Manager before you upgrade Cryptographic Security Platform Vault.

You can upgrade from Cryptographic Security Platform Vault 5.5.1 to 10.6.1. To do so, you upgrade from 5.5.1 to 10.0, then upgrade from 10.0 to 10.1.1, then from 10.1.1 to 10.2, then from 10.2 to 10.3.1, then to 10.4.1, 10.4.1.1, or 10.4.3, and then to 10.6.1.

For details on upgrading earlier versions, please see the version of the documentation that you are upgrading to. For example, if you need to upgrade from 5.5.1 to 10.0, see the KeyControl 10.0 documentation.

> Note: Because the OS for Cryptographic Security Platform Vault was changed in 10.4.1, if you upgrade from 10.3.3 or earlier, the process is a migration method rather than the standard upgrade procedure. Please be sure to review the Installation and Upgrade Guide for 10.4.3 before you start the upgrade. We recommend that you migrate to version 10.4.3 and then upgrade directly to 10.6.1.

CSP Vault Upgrade Requirements

Important:

- **You must upgrade the Cryptographic Security Platform Compliance Manager before you upgrade Cryptographic Security Platform Vault.**

- The CSP Vault Management Appliance and all CSP Vaults must be connected to the CSP Compliance Manager and must have a valid unexpired license, as well as usage within the limits for each category, before you start the upgrade.
  Note:
  - If your vaults are not connected to the CSP Compliance Manager, you can connect them after you have upgraded CSP Compliance Manager to 10.5.1. For versions 10.4.5 and above, follow the directions in Connecting CSP Vault and CSP Compliance Manager. For CSP Vault version 10.4.3, you will need to download the JSON file and then copy the Compliance Manager ID and the App Link Token from the JSON file. To do this:
    i. Download the JSON file from the CSP Compliance Manager webGUI.
    ii. Open the JSON file with a text editor. The beginning will look similar to the following text:
    "appLinkToken":
    "NkFGNDM0MUMzRDI4NEExNzQ5NDYzMDlENjE4QjZGREQ0Q0Y5NjlEQzg5MDgxRUJDRDBBQzY1RTFBQjU2OTZGREEwNzc0NjhERjVCRDQwOEZBRDc0ODM4QTlBRjFCRkY5NTVGMjNDMkUwNDA4QkQ3NTc1MzQ3MDk3QjVBMTU1MDZCQkQ4QUFCNTA4QzJBQkMxMTlBQ0U2MTQyRTRCQUIwRkZDOTc4ODY0QjRCRDM1NDgyRjcwMUM4MDcyQjg5Q0IwREMyMDk5NkM4NjZFQjRGQkYzN0M1MUFCOEUwRjMxMzBGRkQ2MUNGRDQ0QTY2NkRBMjhENzA4RDQzQjMwMTJBNkMyQjA5QkZCRTIzRkJERUE5QjUxMjcyRUU1QThBMUVB",
    "kcmId": "10.1.232.31",
    "sslVerify": true,
    "applicationId": "cbe4d5a1-a25c-4721-a95f-5981522b7ef5",
    "rootCertificate": "-----BEGIN CERTIFICATE-----\nMIIGATCCA+mgAwIBAgIEaYuG/jANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJV\n
    iii. Copy the text for the `appLinkToken` and paste it in the Token field in the KeyControl webGUI.
    iv. Copy the `applicationId` and paste it in the KeyControl Compliance Manager ID field in the KeyControl webGUI.
    v. Click **Connect**.
  - If you are using BYOK or TDE, you may encounter an error message during the upgrade process similar to: The upgrade can not be started: ["Cloud Keys Vault 'BYOK_Dev_Vault' Cloud Key(s) license entitlement above limit (count: 479, limit: 0)."]. The message text will vary, but the count will be non-zero and the limit zero.
    If this happens, open your Cryptographic Security Platform Compliance Manager to the collection that contains the Vault where you received the error messages. Navigate to the Licenses page and remove all but one license file (CSP Compliance Manager will not let you remove all licenses). Add those licenses back in, then remove and add back the last license file.
    After you complete that step, restart the upgrade.
- If you have a multi-node cluster with passphrase-based startup authentication, you cannot upgrade directly to 10.5.1. You must either disable the startup authentication or reduce the cluster to a standalone node before you upgrade.
- If you have just upgraded from a previous version, and want to upgrade to a newer version, you may see a message that reads: Ongoing Encrypt on Cryptographic Security Platform Vault system device - Try again later. In this case, the internal processing will take about 30 minutes to complete before you can continue.

After you upgrade your Cryptographic Security Platform Vault nodes, we strongly recommend that you also upgrade the Policy Agents running on all VMs registered with Cryptographic Security Platform Vault. For details, see Policy Agent Upgrade Requirements.

Upgrading CSP Vault to 10.6.1

If your Cryptographic Security Platform Vault nodes are running version 10.4.3 or later, you can use the Cryptographic Security Platform Vault Management webGUI to upgrade any node in the cluster and Cryptographic Security Platform Vault will automatically upgrade the other nodes one at a time until all nodes have been upgraded. By doing sequential upgrades, Cryptographic Security Platform Vault ensures that at least one node in the cluster remains available during the entire upgrade process.

Important: If you are using HSM Root-of-Trust mode with password, you must enter the password on each node during upgrade.

You can use this procedure for all installations of Cryptographic Security Platform Vault, including AWS, Azure, and GCP.

> Note: Any new features in the Cryptographic Security Platform Vault release will *not* be available until all nodes in the cluster have been upgraded.

Before You Begin

- Make sure that the Cryptographic Security Platform Vault nodes can communicate with one another on port `TCP/8443` and `TCP/5432`. For details, see Network requirements.
- Entrust recommends that you back up your Cryptographic Security Platform Vault cluster before you upgrade it. For details, see Backing Up CSP Vault Through the webGUI
- Please download your Admin Key and store it in a safe place before you upgrade. If Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data. For details, see Downloading Your Admin Key Part.
- We recommend that you enable the support login on all cluster nodes before you start the upgrade. For details, see Enabling or Disabling the Support Login .
- Make sure your internet connection to the Cryptographic Security Platform Vault node is as fast and as stable as possible. To begin the upgrade, you need to upload the upgrade ISO image to the Cryptographic Security Platform Vault node in one continuous session. If the upload times out or if connectivity to the Cryptographic Security Platform Vault node is lost during the upload, you will see error messages in Cryptographic Security Platform Vault and you must re-upload the file from scratch. Cryptographic Security Platform Vault *cannot* resume the upload from where it left off during a previous session.

Procedure

1. Sign on to the Cryptographic Security Platform Vault Management webGUI with Domain and Security Admin privileges.
2. In the top right, click the **Appliance Management** link.
3. In the top menu bar, click **Cluster** and make sure the **Status** of the cluster is **Healthy**. If it is not, you must resolve those issues before you can upgrade the cluster.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **System Upgrade**.
6. Click **Browse**, navigate to the Entrust ISO upgrade file, and click **Open**.
   Important: Cryptographic Security Platform Vault now has separate ISO files for installation and upgrade. Please ensure that you use the ISO upgrade file.
7. Click **Upload File**. If the **Upload File** button is not active, make sure that you have selected an ISO file and that the cluster is healthy.
   After Cryptographic Security Platform Vault uploads and validates the ISO file, Cryptographic Security Platform Vault begins the automatic upgrade process by copying the ISO file from the current node to all of the other Cryptographic Security Platform Vault nodes in the cluster. After the ISO file has been copied, Cryptographic Security Platform Vault displays a Success message. Click **Close** to continue with the upgrade.

Cryptographic Security Platform Vault displays a status message stating that the upgrade is in process along with a **Cancel Upgrade** button in case you want to stop the process.
During this time you can continue to use Cryptographic Security Platform Vault as normal, including changing all configuration options and adding or removing VMs. When Cryptographic Security Platform Vault is ready to upgrade all nodes in the cluster, it displays the **Finish Upgrade** button.

8. Click **Finish Upgrade**.
   Note: Ensure you are still on the same node where you clicked **Upgrade File**.
   Cryptographic Security Platform Vault displays a message stating that the cluster will be put into maintenance mode during this procedure and that all nodes will be rebooted. While in maintenance mode, Cryptographic Security Platform Vault can still service key requests from the registered VMs, but no Cryptographic Security Platform Vault configuration changes can be made and no new VMs can be added.
9. Click **Proceed**.
   Cryptographic Security Platform Vault displays a status message stating that the cluster nodes are being rebooted. It may take a while for this process to run on all nodes except for the current node. When all of the other nodes have been upgraded and are back online, Cryptographic Security Platform Vault reboots the current node to finish the upgrade process on that node. At this point, you will be automatically logged out of the Cryptographic Security Platform Vault Management webGUI on that node. You can monitor the progress on the Cryptographic Security Platform Vault Management webGUI of the other nodes. This again may take a while to complete.
   When any node is being upgraded, if you have access to the Cryptographic Security Platform Vault System Console, you can view the upgrade messages.
   Note: When Cryptographic Security Platform Vault reboots the current node, you may see a message that the application cannot connect to the server, then browser page may display a "connection refused" message. Wait a few moments for the node to finish rebooting, then refresh your browser page. You should see the Cryptographic Security Platform Vault Login page.
   Beginning with 10.2, Cryptographic Security Platform Vault has changed the login experience. You can now switch between the Cryptographic Security Platform Vault Management webGUI and the Cryptographic Security Platform Vault Appliance Management webGUI in the same browser with one login. When you log in, click the Switch to **Appliance Management** link at the top right side of the web page to switch.
10. To verify the upgrade, return to **Settings > System Upgrade** and verify the settings for **Current Version** and **Previous Version**.

9 Installing Policy Agent

Preparing to Install the Policy Agent

Before you can install the Policy Agent on Linux or Windows, you must complete the following:

1. Determine whether you want to use the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption.
2. In the Cryptographic Security Platform Vault Management webGUI select **Create Vault** and follow the steps in Creating a Vault.
   You must create either the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption.
3. Create a Cloud Admin Group. For more information, see Cloud Admin Groups.
4. Create a Cloud VM Set for your vault. For more information, see see Creating a Cloud VM Set for the CSP Vault for Databases or Creating a Cloud VM Set for the CSP Vault for VM Encryption.

Linux Policy Agent Installation

Linux Policy Agent Installation Overview

The Entrust Policy Agent is a software module that runs inside Windows and Linux operating systems that provides encryption of virtual disks and individual files. All VMs that have the Policy Agent installed can also securely share encrypted files and disks. When a user attempts to access an encrypted disk, the Policy Agent queries Cryptographic Security Platform Vault to validate the request, and returns the information to the user if Cryptographic Security Platform Vault authorizes the request.

You must install a copy of the Policy Agent in each VM you want to encrypt with Cryptographic Security Platform Vault.

Linux Installation Prerequisites

- Make sure the version of Linux running on the target system is supported for data encryption. For details, see Supported platforms.
- Make sure the default language for the Linux operating system is English. The Entrust Policy Agent uses scripts that parse the output of Linux commands, and those scripts may give unexpected results if the command output is in a language other than English.
- Make sure that the `tar` utility is installed. If you see this error, then `tar` is not installed:
  `Uncompressing hcs-client-agent-10.5.1-550001852.run ... Extraction failed.`
- Make sure that Entrust Cryptographic Security Platform Vault is installed and the cluster is configured properly as described in Initializing the CSP Vault Management webGUI. The cluster must be healthy. You cannot register the Policy Agent with a degraded Cryptographic Security Platform Vault cluster.
- Have the following information available:

    - The IP addresses of all Cryptographic Security Platform Vault nodes with which you want to register the Policy Agent, or one IP address and the name of the Cluster Node Mapping you want to use on this VM. Registering the Policy Agent with multiple Cryptographic Security Platform Vault nodes provides a failover mechanism in case one of the Cryptographic Security Platform Vault nodes is unreachable.
    - The credentials for a Cryptographic Security Platform Vault webGUI user account with Cloud Admin privileges.
    - The name of the Cryptographic Security Platform Vault Cloud VM Set with which you want to associate the VM. You cannot encrypt the disks or drives until the VM has been registered with a Cloud VM Set in Cryptographic Security Platform Vault. For details, see the Administration Guide.
- Select an authentication method. The options are:
    - **Standard Authentication** — This is the most secure authentication method. You create a certificate in the Cryptographic Security Platform Vault webGUI which you then copy to the target system. After you install the Policy Agent software, you specify the name and location of the certificate file during registration. You also create a passphrase during the Policy Agent registration that you must then enter in the Cryptographic Security Platform Vault webGUI.
    - **Simplified Authentication** — This method involves authenticating the VM with Cryptographic Security Platform Vault through the VM itself. It allows you to skip downloading a certificate and logging into Cryptographic Security Platform Vault during the authentication process, but it does require you to enter the Cryptographic Security Platform Vault credentials directly into the VM and to have a Cloud VM Set already created. You should only use this method if your VM is secure.
    - **Automated Authentication** — This method involves adding the Cryptographic Security Platform Vault username and password on the `hcl` command line using the `hcl register -a` command. This method is the least secure and should be used with caution due to the fact that the Cryptographic Security Platform Vault username and password must be included on the command line or in the script.
- **RHEL 10 Caveats**—If you plan to use RHEL 10 with the Linux Policy Agent, please be aware of the following:
    - The 'htroot setup' job will fail if network is set to DHCP. This is because system device encryption is not supported with DHCP. To fix this issue, please use static IP configuration during setup.
    - The 'htdrv prepare' job may fail to install the EPEL package. To fix this issue, run the following command manually:
      `rpm -Uvh "https://dl.fedoraproject.org/pub/epel/epel-release-latest-10.noarch.rpm"`
      Then you can rerun the 'htdrv prepare' job.
    - The upgrade process using Leaap will fail if the root disk is encrypted. To fix this issue, boot into RHEL 9 from the GRUB menu to rescue the VM.
      To avoid this issue do the following:
        i. Decrypt the root disk before upgrading.
        ii. Perform a clean upgrade to RHEL 10.
        iii. Re-encrypt the root disk after the upgrade is complete.

Installing the Policy Agent on Linux

See below for installing the Policy Agent on Linux.

- Downloading the installation file

> Make sure you have completed the prerequisites described in Linux Installation Prerequisites.

Downloading the installation file

See below for installing the Policy Agent installation file.

To download the Policy Agent installation file

1. Log in to the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the following file:

```
hcs-client-agent-rel.number-build.number.run
```

Creating a certificate for the registration process

Create a certificate that you can install on the VM and use during the registration process.

> Skip this section if you want to use Simplified or Automated Authentication.

To create a certificate for the registration process

1. Select the Cloud VM Set with which you want to associate the VM.
2. Click **Actions > Create New Certificate**.
3. If desired, enter a passphrase for the certificate. If you enter a passphrase here, you will need to enter that passphrase when you install the certificate on the VM.
4. Enter a date on which this certificate should expire.
5. Click **Create**. Cryptographic Security Platform Vault downloads a `.cert` file to the default download location.

> Do not rename the downloaded certificate. The certificate name includes additional information, and a renamed certificate will fail.

6. Log in to the target system as `root`.
7. Go the directory containing the following file:

   a. `hcs-client-agent-rel.number-build.number.run`

8. `# sh ./hcs-client-agent-rel.number-build.number.run [install -y] [-P Installation_Path]`
   Where `-y` tells the installer to use the default installation directory (`/opt/hcs`) without prompting, and -P specifies the installation directory.
   Important:
   - `hcs-client-agent-rel.number-build.number.run` extracts itself to the `/tmp` directory. Make sure that you have executable permissions to `/tmp`.
   - If you run the installer and get the following error:
     `./install.sh: Permission denied`

then you can must use a different directory for the temporary directory using the environment variable TMPDIR as follows:

```
#> TMPDIR=$HOME
```

When uninstalling the Linux Policy Agent you will also need to use a different directory.

The following examples both install the Policy Agent in the directory `/opt/hcs`, but in the first one the user is prompted for the installation directory and in the second the installer uses that directory without prompting:

```
# sh ./hcs-client-agent-10.5.1-12345.run
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.....
HyTrust Agent will be installed in /opt/hcs
Specify location for installing HyTrust Agent (/opt/hcs): <Enter>
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
 — Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

```
# sh ./hcs-client-agent-10.5.1-12345.run install -y
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.....
HyTrust Agent will be installed in /opt/hcs
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
 — Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

The following example installs the Policy Agent in the specified directory `/opt/test` without prompting:

```
# sh ./hcs-client-agent-10.5.1-12345.run install -y -P /opt/test
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.....
HyTrust Agent will be installed in /opt/test
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
 — Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

9. Register the VM with Cryptographic Security Platform Vault using the following command:

   `hcl register [-a] [-h vm-name] [-d "vm-description"] [-p cert-passphrase] [-o one-time-passphrase] [-z cvm-set] [-v vault_id] [-n mapping-name] [-N] kc-hostname[:port],kc-hostname2[:port],... [cert-file.cert ]`

   where:

- `-a` —Indicates that you want to authenticate the VM through the command line or the script instead of through a certificate file. Use this option if you are using Simplified or Automated Authentication. If you created a certificate in Cryptographic Security Platform Vault, omit this option and specify the certificate name in `cert-file.cert` .
- `-c` —Allows you to register this VM as clone of the original VM.
- `-h` —The name of the VM that will be displayed in the Cryptographic Security Platform Vault webGUI (Default: hostname).
- `-d` —A description of the VM that will be displayed in the Cryptographic Security Platform Vault webGUI.
- `-p` —The passphrase assigned to the certificate when it was created. If you do not specify this parameter and the certificate has an associated passphrase, the registration process prompts you for the passphrase. Applies to Standard Authentication only.
- `-v` —The Vault ID of the Vault that will be displayed in Vault Management. If you do not specify the vault_id, you will be asked to enter vault_id ..
- `-o` —The one-time passphrase that will be used to encrypt the initial communication between this VM and the existing Cryptographic Security Platform Vault cluster. If you do not specify this parameter, the registration process prompts you for the one-time passphrase. Applies to Standard Authentication only.
  Note: The passphrase is valid for 15 minutes from the time it is created. Make sure you authenticate the VM in Cryptographic Security Platform Vault during this time. Authentication will fail after the passphrase has expired.
- `-z` —The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault cluster to which you want to assign this VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `-n` —The name of the Cluster Node Mapping that you want to associate with this VM. If you do not specify this option and one or more Cluster Node Mappings have been configured, the Policy Agent prompts you to select a Node Mapping from the list. If you do not want to use a Node Mapping, you must manually respond to this prompt. This option is mutually exclusive with the `-N` option, described below, and it requires that the `-a` option must be specified on the `hcl register` command.
- `-N` —Tells the Policy Agent that you do *not* want to use a Cluster Node Mapping, even if one is available. If you specify both `-N` and `-n` , the Policy Agent ignores the `-n` option and does *not* assign a Node Mapping to the VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `kc-hostname[:port],kc-hostname2[:port],...` (required) — The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443).
  If you are using the `-n` option to specify a Cluster Node Mapping, this IP address will be the Cryptographic Security Platform Vault node that the VM contacts to retrieve the Node Mapping information. After the Node Mapping has been retrieved, the Policy Agent ignores any other IP addresses in this list and only registers the VM with the Cryptographic Security Platform Vault nodes in the contained in the Node Mapping.
- `cert-file.cert` —The name of the certificate file you copied to the target system if you are using Standard Authentication. If you are running the `hcl register` command from a directory other than the one where the `.cert` file resides, specify the full path to the `.cert` file as part of this option. If you

did not create a certificate file in Cryptographic Security Platform Vault, omit this option and use the `-a` option instead.

Registration Examples with Standard Authentication

If the VM name is "hq-vm-4", the description is "HQ Linux Server Alpha", and you want to register it using Standard Authentication with two Cryptographic Security Platform Vault nodes at 10.238.32.74 and 10.238.32.75, you would enter:

```
# hcl register -h hq-vm-4 -d "HQ Linux Server Alpha" 10.238.32.74,10.238.32.75 \
    ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert
You need to specify a passphrase that will be used for authentication
Enter passphrase (min 16 characters): passphrase16chars

Registered as hq-vm-4 with node(s) 10.238.32.74,10.238.32.75
Please login to the node to complete the authentication of this node
```

To register the VM in a single command where the `.cert` file resides in the directory `/install/hytrust/cert`, you would enter:

```
# hcl register -h hq-vm-4 -d "HQ Linux Server Alpha" -p certpassphrase \
    -o onetimepassword16chrsmin 10.238.32.74,10.238.32.75 \
    ./install/hytrust/cert/ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert

Registered as hq-vm-4 with node(s) 10.238.32.74,10.238.32.75
Please login to the node to complete the authentication of this node
```

Registration Examples with Simplified Authentication

In this example, the VM name is "hq-vm-4", the description is "HQ Linux Server Alpha", and the Cryptographic Security Platform Vault node you want to use is at 10.238.66.250. You want to be prompted for the Cryptographic Security Platform Vault Cloud Admin account information, the Cloud VM Set, and the Cluster Node Mapping.

In this case, you would enter:

```
# hcl register -a -h hq-vm-4 -d "HQ Linux Server Alpha" 10.238.66.250

Do you want to register into a Vault? (y/n) y
Please provide the vaultID
vaultid: d84243e7-d359-4179-9530-3497434e3192
Please provide the login details
username: CloudAdmin
password:

Available Cloud VM Sets
--------------------------------------------------------------------------------
SF-Datacenter
--------------------------------------------------------------------------------

Please specify Cloud VM Set to which this VM should be added: SF-Datacenter
Registered as hq-vm-4 with node(s) 10.238.66.250

Completing authentication for hq-vm-4 on node(s) 10.238.66.250

Authentication complete, machine ready to use
```

Getting Mapping information

This VM can be added to one of the following Mappings
---
1 : SF-Datacenter-Map
2 : West-Coast-Map

Please select a numeric Mapping ID (0 to skip): 1
Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated list with nodes 10.238.66.250:443,10.238.66.251:443

To specify the name, description, Cloud VM Set and Cluster Node Mapping in a single command, you would enter:

hcl register -a -h hq-vm-4 -v d84243e7-d359-4179-9530-3497434e3192 -d "HQ Linux Server Alpha" -z SF-Datacenter -n SF-Datacenter-Map 10.238.66.250

Please provide the login details
username: CloudAdmin
password:
Registered as hq-vm-4 with node(s) 10.238.66.250

Completing authentication for hq-vm-4 on node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting Mapping information

Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated list with nodes 10.238.66.250:443,10.238.66.251:443

Registration Example with Automated Authentication

If the VM name is "hq-vm-4", the description is "HQ Linux Server Alpha", and you want to register it using Automated Authentication with two Cryptographic Security Platform Vault nodes at 10.238.32.74 and 10.238.32.75, you would create a registration script containing the following command:

hcl register -a -h hq-vm-4 -d "HQ Linux Server Alpha" -v d84243e7-d359-4179-9530-3497434e3192 -u htcloudadmin -s 'DogDays123!' \
    10.238.32.74,10.238.32.75
Certificate passphrase might be required
Certificate successfully unpacked

Registered as hq-vm-4 with node(s) 10.238.32.74,10.238.32.75
Completing authentication for hq-vm-4 on node(s) 10.238.32.74,10.238.32.75
Authentication complete, machine ready to use

What to Do Next

If you used Standard Authentication, authenticate the VM with Cryptographic Security Platform Vault as described in Authenticating a New VM. If you used Simplified or Automated Authentication, encrypt the drive as described in Data Encryption Overview.

Authenticating a New VM

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Unauthenticated VMs** tab.
4. Select the VM you want to authenticate.
5. Click **Actions > Authenticate**.
6. Enter the system passphrase at the prompt and click **Authenticate**. This passphrase must exactly match the passphrase that was specified when the new VM was registered. The passphrase is case-sensitive.
7. Click on the VM to verify that the VM is reachable and the VM details match what you expect.

Windows Policy Agent Installation

Windows Installation Prerequisites

- Make sure the version of Windows running on the target system is supported for data encryption. If you want to encrypt the boot drive, make sure the Windows version is supported for boot drive encryption as well. For details, see Supported platforms.
- Make sure the default language for the Windows operating system is English. The Entrust Policy Agent uses scripts that parse the output of Windows commands, and those scripts may give unexpected results if the command output is in a language other than English.
- Make sure that the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases is installed and the cluster is configured properly as described in the Administration Guide. The cluster must be healthy. You cannot register the Policy Agent with a degraded cluster.
- Make sure the target system is partitioned correctly and you know which partition you want to encrypt. In addition, the partition must be assigned a drive letter or folder mount through the Windows Disk Manager. For details, see your Windows documentation.
- Make sure that the Microsoft .NET framework 4.8.0 or higher is installed on the target system. For more information, see https://dotnet.microsoft.com/en-us/download/dotnet-framework/net481.
  Note: The Microsoft .NET framework is required to use the Policy Agent GUI. If not installed, you will need to use the CLI.
- If you want to encrypt the boot drive, see the prerequisites in Windows Boot Drive Installation Prerequisites.

Windows Boot Drive Installation Prerequisites

The Entrust Policy Agent supports encryption for Windows MBR and GPT boot disks, including any GPT boot disks that use UEFI Secure Boot, as long as those boot disks meet the following requirements.

Important: UEFI and Secure Boot is only supported with VMware ESXi. It is not supported on AWS, Azure, or GCP.

For details on boot drive encryption, see Windows Boot Drive Encryption.

- The encrypted boot partition must be on the Windows `C:` drive. Although Windows itself can boot from alternate drive letters, the boot volume can only be encrypted if it is the `C:` drive or if it is mapped to `C:`. The Bootloader is automatically assigned a drive letter during installation. This default drive letter can be changed using the Windows Disk Manager after the Bootloader has been installed.
- The Bootloader requires a Windows System Reserved Partition (SRP). We will create an SRP if one does not already exist.
  The Bootloader SRP requires roughly 350 MB on Windows 2016 and above, and roughly 100 MB on Windows 10. As part of the installation process, the boot drive will shrink to free up space for the Bootloader (and Windows SRP if one does not already exist). If there is insufficient space on the boot drive, the Bootloader will fail to install.
  Note: If the Bootloader SRP has less than 50 MB free space, Cryptographic Security Platform Vault generates an alert every six hours until the issue is resolved.
- The SRP and the boot partition must both reside on `Harddisk0` (Disk 1). You cannot encrypt a boot partition that resides on any other disk, or split the SRP and the boot partition across disks.
- The boot disk must have at least 1 MB of free space at the beginning of the disk that Cryptographic Security Platform Vault can use to store encryption metadata. If this free space is not available, boot drive encryption will fail.
- If the VM is associated with a Cloud VM Set that is controlled by a Key Encryption Key (KEK), the HSM must be available before you can encrypt the root drive on the VM. For more information, see KEKs with Cloud VM Sets.
- The Disk Defragmenter service on the target server must be enabled before installing the Policy Agent software.
- The user account used for installing the software must have **SeRestorePrivilege** and **SeTakeOwnershipPrivilege**.
- For GPT boot disks:
  - The GPT disk must be running Windows Server 2016, Windows Server 2019, Windows Server 2022, or Windows 10.
  - The boot partition must be one of the first four partitions on the disk.
    Tip: If you try to encrypt the boot disk and the boot partition is not one of the first four partitions, the encryption will fail with the error "Maximum supported encrypted partition limit exceeded."
  - If you want to extend the boot partition, you must use the `hcl extend` command. For details, see Disk Size Management in Windows.

Installing Interactively on Windows

This procedure described how to install the Entrust Policy Agent by interacting with the installer on the Windows system. For details about installing the Policy Agent silently, see Installing Silently on Windows.

Before You Begin

- Make sure you have completed the prerequisites in Windows Installation Prerequisites.
- Make sure you have the credentials for a Windows user account with Administrator privileges.
- If you plan to download the Policy Agent installation file on Windows 10 from the Microsoft Edge browser while logged in with the BUILTIN\Administrator account, make sure that User Account Control (UAC) is enabled for the BUILTIN\Administrator account. Alternatively, you can set the integrity level for the installer to high after you have downloaded it. For details, see the Microsoft Windows 10 documentation.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to encrypt.
6. Log into the target Windows system as an Administrator.
7. Navigate to the directory in which you placed the `hcs-client-agent-rel.number-build.number.exe` file and run the installer.
8. On the **Welcome** page of the Setup Wizard, click **Next**.
9. On the **License Agreement** page, review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
10. On the **Choose Install Location** page, select the folder in which Policy Agent will be installed.
    Note: You must install Policy Agent in a folder on the `C:` drive.
11. In the **Choose Components** page, review the setting of the **HT Bootloader** option.
    If you want to encrypt the boot drive on this system now or in the future, make sure this option is selected. If you do not need to encrypt the boot drive, make sure this check box is cleared. The Bootloader is only supported for the Cryptographic Security Platform Vault for VM Encryption.
    Note: If you do not install the Entrust Bootloader now, you can do so later if needed. For details, see Installing the Bootloader After the Policy Agent Is Installed.
12. If the **HT Bootloader** option is *not* selected:
    a. Click **Install**.
    b. On the Completing the Entrust Setup Wizard page, select **Reboot Now** and click **Finish**.
13. If the **HT Bootloader** option *is* selected:
    a. Click **Next**.
    b. On the Drive and Network Configuration page, select the drive letter and the network that the Entrust Bootloader should use when connecting to Cryptographic Security Platform Vault. By default, this dialog box shows the current DeviceID (a unique integer) and ConnectionID from `WMI class Win32_NetworkAdapter` for the selected network interface.
    c. When you are finished, click **Install**.
    d. If prompted, click **Yes** to remove any existing Bootloader partitions.
    e. On the Completing the Setup Wizard page, select **Reboot Now** and click **Finish**.
    f. The machine will reboot several times to finish the installation. After the machine has finished booting, copy the `id_rsa` key file to another location in case you ever need to access the Entrust Bootloader Debug Console using SSH.
    Tip: You can download the `id_rsa` key file using the Cryptographic Security Platform Vault for VM Encryption webGUI after the boot drive has been encrypted. To do so, log into the Cryptographic Security Platform Vault for VM Encryption webGUI, click **Workloads** and go to the **VMs** tab. Select the appropriate VM, then select **Actions > Download Bootloader SSH Key**.

What to Do Next

Register the VM as described in Registering the Policy Agent Using the Entrust Policy Agent GUI or Registering the Policy Agent from the Windows Command Line.

Installing Silently on Windows

This procedure describes how to install the Entrust Policy Agent silently on Windows using a command line script. For details about installing the Policy Agent through an interactive GUI, see Installing Interactively on Windows.

Note: The Policy Agent can only be installed on the Windows system (C:) drive, not a data drive.

Before You Begin

- Make sure you have completed the prerequisites in Windows Installation Prerequisites.
- Make sure you have the credentials for a Windows user account with Administrator privileges.
- If you plan to download the Policy Agent installation file on Windows 10 from the Microsoft Edge browser while logged in with the BUILTIN\Administrator account, make sure that User Account Control (UAC) is enabled for the BUILTIN\Administrator account. Alternatively, you can set the integrity level for the installer to high after you have downloaded it. For details, see the Microsoft Windows 10 documentation.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to encrypt.
6. If your system contains multiple network adapters and you want to specify the adapter that Cryptographic Security Platform Vault should use, do the following:
   a. Enter the command `hcs-client-agent-rel.number-build.number.exe /NLIST`. Cryptographic Security Platform Vault writes the list to the file `HTIfaceList` in the same directory as the installer executable.
   b. Open `HTIfaceList` and determine the index of the adapter you want to use.
   c. Specify that index using the `/NET` switch as described in the next step.
7. Run `hcs-client-agent-rel.number-build.number.exe` using the following switches. All switches are case-sensitive and must be entered in upper-case. The installer ignores any unsupported switches.

Switch	Description
/S	Required. Tells Windows to run the installer silently.
/NORB	Do not reboot automatically. Required if you want to check the final state of installation, which is explained in the following step.
Windows Bootloader Switches	
/NOBL	Do not install the Windows Bootloader. The default is to install the Bootloader.
/NLIST	List of network adapters with an index that can be used with the `/NET` switch. This does not cause actual installation.

Switch	Description
/NET=*n*	Use adapter *n* with its current settings as the primary network interface for the Entrust Bootloader, where *n* is the DeviceID of any of the network adapters listed by `/NLIST`. If this switch is not specified, the first network adapter is used by default. This is equivalent to specifying `/NET=1`.
/DRIVE=*d*	Assign drive letter *d* to the Bootloader partition. The drive letter is not case-sensitve.
/NORM	Do not delete HTBOOTLDR partition left by an older installation. By default, old HTBOOTLDR partitions are deleted.

For example, if you want to run `hcs-client-agent-10.5.1-12345.exe` silently, assign the drive letter D to the Bootloader, and not reboot automatically after the install runs, you would enter:
`C:\hytrust\installer\dir> hcs-client-agent-10.5.1-12345.exe /S /DRIVE=D /NORB`

8. If you specified the /NORB switch and you want to check the success of the installation, look at the files generated by the installer. These files will be placed in the same directory as the `.exe` file. The files are:
   - `HTDone` —This indicates the installation ended. You should poll for creation of this file to ensure that the installer process finished. If no other file is created, it means that the installation completed successfully.
     Note: Boot drive encryption is not available until AFTER a successful installation and reboot.
   - `HTError` —The installation failed. This file contains the error string.
   - `HTBLError` —Entrust Bootloader installation failed, but the rest of the installation succeeded. This file contains the error string.
   - `HTRetryOnReboot` —If this file is present, the installation was not a failure, but it needs a reboot. To complete the installation, reboot and run the installer again.
9. If you specified the /NORB switch, reboot the Windows system to complete the installation.

What to Do Next

Register the VM with Cryptographic Security Platform Vault as described in Registering the Policy Agent Using the Entrust Policy Agent GUI or Registering the Policy Agent from the Windows Command Line.

Registering the Policy Agent Using the Entrust Policy Agent GUI

Before You Begin

Make sure that you know:

- The IP address of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node with which you want to register the Policy Agent.
- The login credentials for a Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account with Cloud Admin privileges.
- The name of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases Cloud VM Set with which you want to associate the VM. You cannot encrypt the drive until it has been associated with a Cloud VM Set. For details, see Creating a Cloud VM Set for the CSP Vault for Databases or Creating a Cloud VM Set for the CSP Vault for VM Encryption.

Procedure

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hcIGUI` command.
3. Click **Register**.
4. In the **Register with a KeyControl Server** dialog box, enter the following information:

Field	Required ?	Description
KeyControl Name / IP	Yes	The IP address of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node with which you want to register this system. Only the IP address is required. Do not enter the full URL.
KeyControl Port	Yes	The Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node port. The default is 443.
Username	Yes	The user name for a Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account with Cloud Admin privileges.
Password	Yes	The password for the specified Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account.
Vault ID	Yes	The Vault ID of the Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI. The Vault ID is located on the About page. Click on your account name in the top right-hand corner or the vault, then select About.
Cloud VM Set	Yes	The name of the Cloud VM Set to which you want to add this VM.
VM Name	Yes	The name for the system that will be displayed in the Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI. The default is VM hostname.
Description	No	A description for the VM that will be displayed in the Cryptographic Security Platform Vault webGUI or Cryptographic Security Platform Vault for Databases webGUI.

Note: The VM name, description, and Cloud VM Set can also be set in the CSP Vault for VM Encryption webGUI or CSP Vault for Databases webGUI.

5. When you are finished, click **Register**.

6. Click **OK** at the Registration Successful prompt.

What to Do Next

Encrypt the drive as described in Data Encryption and Windows Boot Drive Encryption.

Registering the Policy Agent from the Windows Command Line

Before You Begin

Make sure that you know:

- The VM Encryption vault details. This is the vault you configured during the initial set up. See the Administration Guide.
- The IP addresses of the Cryptographic Security Platform Vault for VM Encryption node with which you want to register the Policy Agent.
- The login credentials for a Cryptographic Security Platform Vault for VM Encryption account with Cloud Admin privileges.
- The name of the Cryptographic Security Platform Vault for VM Encryption Cloud VM Set with which you want to associate the VM. You cannot encrypt the drive until it has been associated with a Cloud VM Set in Cryptographic Security Platform Vault for VM Encryption. For details, see the Administration Guide.

Procedure

1. When you register the VM, you can either specify the Cloud VM Set you want to use interactively during the registration process or you can create a certificate for that Cloud VM Set in the Cryptographic Security Platform Vault for VM Encryption webGUI and then use that certificate during the registration process.
   To create the Cloud VM Set certificate:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
   b. In the top menu bar, click **Workloads**.
   c. On the **VM Sets** tab, select the Cloud VM Set with which you want to associate the VM.
   d. Click **Actions > Create New Certificate**.
   e. If desired, enter a passphrase for the certificate. If you enter a passphrase here, you will need to enter that passphrase when you use the certificate on the VM.
   f. Enter a date on which this certificate should expire.
   g. Click **Create**. The Cryptographic Security Platform Vault for VM Encryption downloads a `.cert` file to the default download location.
   Important: Do not rename the downloaded certificate. The name of the certificate has additional information, and a renamed certificate will fail.
   h. If necessary, copy the `.cert` file to the Windows VM.
2. Log into the VM using an account with Administrator privileges.
3. Open a Windows Command prompt and navigate to the directory in which you placed the `.cert` file. If you do not have a `.cert` file, you can register the VM from the any directory.
4. Register the VM with Cryptographic Security Platform Vault for VM Encryption using the following command:
   `hcl register [-a] [-h vm-name] [-d "vm-description"] [-p cert-passphrase] [-o one-time-passphrase] [-z cvm-set] [-v vault_id] [-n mapping-name] [-N] kc-hostname[:port],kc-hostname2[:port],... [cert-file.cert ]`
   where:
   - `-a` — Indicates that you want to authenticate the VM through the command line or the script instead of through a certificate file. Use this option if you are using Simplified or Automated Authentication. If you created a certificate in Cryptographic Security Platform Vault, omit this option and specify the certificate name in `cert-file.cert` .

- `-h` —The name of the VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption (Default: hostname).
- `-d` —A description of the VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption.
- `-p` —The passphrase assigned to the certificate when it was created. If you do not specify this parameter and the certificate has an associated passphrase, the registration process prompts you for the passphrase. Applies to Standard Authentication only.
- `-v` (optional)—The Vault ID of the Vault that will be displayed in Vault Management. If you do not specify vault_id, you will be asked whether you want to enter vault_id or not.
- `-o` —The one-time passphrase that will be used to encrypt the initial communication between this VM and the existing Cryptographic Security Platform Vault for VM Encryption cluster. If you do not specify this parameter, the registration process prompts you for the one-time passphrase. Applies to Standard Authentication only.
  Note: The passphrase is valid for 15 minutes from the time it is created. Make sure you authenticate the VM in Cryptographic Security Platform Vault during this time. Authentication will fail after the passphrase has expired.
- `-z` —The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault for VM Encryption cluster to which you want to assign this VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `-n` — The name of the Cluster Node Mapping that you want to associate with this VM. If you do not specify this option and one or more Cluster Node Mappings have been configured, the Policy Agent prompts you to select a Node Mapping from the list. If you do not want to use a Node Mapping, you must manually respond to this prompt. This option is mutually exclusive with the `-N` option, described below, and it requires that the `-a` option must be specified on the `hcl register` command.
- `-N` —Tells the Policy Agent that you do *not* want to use a Cluster Node Mapping, even if one is available. If you specify both `-N` and `-n`, the Policy Agent ignores the `-n` option and does *not* assign a Node Mapping to the VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `kc-hostname[:port],kc-hostname2[:port],...` (required)—The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443).
  If you are using the `-n` option to specify a Cluster Node Mapping, this IP address will be the Cryptographic Security Platform Vault for VM Encryption node that the VM contacts to retrieve the Node Mapping information. After the Node Mapping has been retrieved, the Policy Agent ignores any other IP addresses in this list and only registers the VM with the Cryptographic Security Platform Vault for VM Encryption nodes in the contained in the Node Mapping.
- *cert-file*`.cert` —The name of the certificate file you copied to the target system if you are using Standard Authentication. If you are running the `hcl register` command from a directory other than the one where the `.cert` file resides, specify the full path to the `.cert` file as part of this option. If you did not create a certificate file in Cryptographic Security Platform Vault for VM Encryption, omit this option and use the `-a` option instead.

Registration Examples with Standard Authentication

If the VM name is "hq-vm-3", the description is "HQ Windows 2022 Server", and you want to register it using Standard Authentication with a Cryptographic Security Platform Vault for VM Encryption node at 10.238.32.74, you would enter:

```
C:\> hcl register -h hq-vm-3 -d "HQ Windows 2022 Server" 10.238.32.74 \F
    ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert
You need to specify a passphrase that will be used for authentication with KeyControl
Enter passphrase (min 16 characters): passphrase16chars

Registered as hq-vm-3 with KeyControl node(s) 10.238.32.74
Please login to the KeyControl node to complete the authentication of this node
```

To register the VM in a single command where the `.cert` file resides in the directory `/install/entrust/cert`, you would enter:

```
C:\> hcl register -h hq-vm-3 -d "HQ Linux Server Alpha" -p certpassphrase \
    -o onetimepassword16chrsmin 10.238.32.74 \
    ./install/entrust/cert/ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert

Registered as hq-vm-3 with KeyControl node(s) 10.238.32.74
Please login to the KeyControl node to complete the authentication of this node
```

Registration Examples with Simplified Authentication

In this example, the VM name is "hq-vm-3", the description is "HQ Windows 2022 Server", and the Cryptographic Security Platform Vault for VM Encryption node you want to use is at 10.238.66.250. You want to be prompted for the Cryptographic Security Platform Vault for VM Encryption Cloud Admin account information, the Cloud VM Set, and the Cluster Node Mapping.

In this case, you would enter:

```
C:\> hcl register -a -h hq-vm-3 -d "HQ Windows 2022 Server" 10.238.66.250

Do you want to register into a Vault?  (y/n) y
Please provide the vaultID
vaultid: d84243e7-d359-4179-9530-3497434e3192
Please provide the login details
username: CloudAdmin
password:

Available Cloud VM Sets
-------------------------------------------------------------------------------
SF-Datacenter
-------------------------------------------------------------------------------

Please specify Cloud VM Set to which this VM should be added: SF-Datacenter
Registered as hq-vm-3 with KeyControl node(s) 10.238.66.250

Completing authentication for hq-vm-3 on KeyControl node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting KeyControl Mapping information


This VM can be added to one of the following KeyControl Mappings
-------------------------------------------------------------------------------
```

1 : SF-Datacenter-Map
2 : West-Coast-Map

Please select a numeric KeyControl Mapping ID (0 to skip): 1
KeyControl Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated KeyControl list with KeyControl nodes 10.238.66.250:443,10.238.66.251:443

To specify the name, description, Cloud VM Set and Cluster Node Mapping in a single command, you would enter:

C:\> hcl register -a -h hq-vm-3 -v d84243e7-d359-4179-9530-3497434e3192 -d "HQ Linux Server Alpha" -z SF-Datacenter -n SF-Datacenter-Map 10.238.66.250

Please provide the KeyControl login details
username: CloudAdmin
password:
Registered as hq-vm-3 with KeyControl node(s) 10.238.66.250

Completing authentication for hq-vm-3 on KeyControl node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting KeyControl Mapping information

KeyControl Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated KeyControl list with KeyControl nodes 10.238.66.250:443,10.238.66.251:443

Registration Example with Automated Authentication

If the VM name is "hq-vm-3", the description is "HQ Windows 2022 Server", and you want to register it using Automated Authentication with a Cryptographic Security Platform Vault node at 10.238.32.74, you would create a registration script containing the following command:

C:\> hcl register -a -h hq-vm-3 -v d84243e7-d359-4179-9530-3497434e3192 -d "HQ Windows 2022 Server" -u htcloudadmin -s 'DogDays123!' \
    10.238.32.74
Certificate passphrase might be required
Certificate successfully unpacked

Registered as hq-vm-4 with KeyControl node(s) 10.238.32.74
Completing authentication for hq-vm-4 on KeyControl node(s) 10.238.32.74
Authentication complete, machine ready to use

What to Do Next

If you used Standard Authentication, authenticate the VM with Cryptographic Security Platform Vault for VM Encryption as described in Authenticating a New VM. If you used Simplified or Automated Authentication, encrypt the drive as described in Data Encryption Overview.

Uninstalling Silently on Windows

Before You Begin

Ensure that the Windows Policy Agent is installed.

Procedure

1. Start Windows command prompt with administrator-level privileges.
2. Run the uninstaller using the following command:
   C:\Program Files\hcs\uninstall.exe "/S _?=c:\Program Files\hcs"
   Note: This command assumes that the Policy Agent is installed in the default location. If you used a different location for your installation directory, please replace the folder paths.

The Windows Policy Agent is uninstalled silently.

10 Upgrading Policy Agent

Policy Agent Upgrade Requirements

The supported upgrade paths for the Policy Agent are listed below.

Important: You may be able to upgrade from an unsupported version, but those versions are not tested. We recommend you only use the supported upgrade paths.

Initial Release	Available Upgrade Paths
10.5.1	10.6.1
10.4.7	10.5.1, 10.6.1
10.4.5	10.4.7, 10.5.1, 10.6.1
10.4.3	10.4.5, 10.4.7, 10.5.1, 10.6.1

Upgrading Policy Agent with the webGUI

Important: You can upgrade the Policy Agent using the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI. This procedure is written using the Cryptographic Security Platform Vault for VM Encryption webGUI, but the steps are the same as for the Cryptographic Security Platform Vault for Databases webGUI.

In order to complete the upgrade, the VM must be rebooted. You can either have this happen automatically during the upgrade procedure or you can tell Cryptographic Security Platform Vault that you want to reboot the VM manually. After you submit the upgrade request, the actual upgrade process will begin the next time that VM heartbeats with Cryptographic Security Platform Vault.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

For older Policy Agents or other upgrade options, see Upgrading the Policy Agent on Linux and Upgrading the Policy Agent on Windows.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. In the top menu bar, click **WORKLOADS**.
3. Select the VM whose Policy Agent you want to upgrade and click the **Expand** button (**>**) at the end of the row.
4. If the Cryptographic Security Platform Vault for VM Encryption webGUI displays a message stating that an updated agent version is available, select **Actions > Upgrade Agent** from the main **Actions** menu.
5. Confirm that you want to upgrade the Policy Agent at the prompt.

6. If you want to have the Policy Agent automatically reboot the VM after the upgrade, click **Yes**. If you want to manually reboot the VM later to finish the upgrade, click **No**.
   Cryptographic Security Platform Vault creates an upgrade task that it communicates to the VM at the VM's next heartbeat. You can view the status of this task on the Dashboard in the Tasks tile. If you want the upgrade to begin immediately, log into the VM as an administrator and use the `hcl heartbeat` command.
7. If you selected No when prompted about automatic reboot, wait until the upgrade task has completed and then reboot the VM to finish the Policy Agent upgrade. The Cryptographic Security Platform Vault for VM Encryption webGUI will continue to display the informational message stating that an updated Policy Agent is available in the VM Details area until the VM is rebooted.
   Note: In some cases, the upgrade might not require a reboot. If the Cryptographic Security Platform Vault for VM Encryption webGUI simply displays the new version, then you do not need to reboot the VM.

Upgrading the Policy Agent on Linux

Before You Begin

- Make sure that you have upgraded your Cryptographic Security Platform Vault nodes before you upgrade your Policy Agents. Registration will fail if the version of the Policy Agent is higher than that of the Cryptographic Security Platform Vault node and your encrypted data may become unavailable.
- Make the upgrade path from your current version to the new version is supported. For details, see Policy Agent Upgrade Requirements.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.run`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.run` to the Linux system that you want to upgrade.
6. Log into the target system as `root`.
7. Run the installer by navigating to the directory containing `hcs-client-agent-rel.number-build.number.run` and entering the command `sh ./hcs-client-agent-rel.number-build.number.run [install -y]`, where `[install -y]` tells the installer to upgrade the agent without prompting.
   For example:

```
# sh ./hcs-client-agent-10.5.1-12345.run
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
HyTrust Agent version 4.1 already installed
Upgrade existing install? (y/n): y
Stopping hcld... done
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
```

— Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful

```
# sh ./hcs-client-agent-10.5.1-12345.run install -y
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
HyTrust Agent version 4.1 already installed
Stopping hcld... done
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
  — Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

8. If you want to verify the version of Policy Agent, enter the following command:
   # hcl version

Upgrading the Policy Agent on Windows

Before You Begin

- Make sure that you have upgraded your Cryptographic Security Platform Vault nodes before you upgrade your Policy Agents. Registration will fail if the version of the Policy Agent is higher than that of the Cryptographic Security Platform Vault node and your encrypted data may become unavailable.
- Make the upgrade path from your current version to the new version is supported. For details, see Policy Agent Upgrade Requirements.
- Make sure that any outstanding encryption or decryption operations are complete on the target system by checking the Cryptographic Security Platform Vault webGUI Dashboard.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to upgrade.
6. Log into the target system as an Administrator.
7. Navigate to the directory in which you placed the `hcs-client-agent-rel.number-build.number.exe` file and run the installer.
8. On the Welcome page of the Entrust Setup Wizard, click **Next**.
9. On the License Agreement page, review the EULA (end user license agreement) and click **I Agree**.
10. In the **Choose Components** page, review the setting of the **HT Bootloader** option.
    If you want to encrypt the boot drive on this system now or in the future, make sure this option is selected.

If you are certain that you will never need to encrypt the boot drive, you can clear this check box.

11. If the **HT Bootloader** option is *not* selected:
    a. Click **Install**.
    b. The installer displays a prompt that the system is going to be upgraded and will require a reboot. Click **Yes** to continue with the upgrade.
12. If the **HT Bootloader** option *is* selected:
    a. Click **Next**.
    b. On the Drive and Network Configuration page, select the drive letter and the network that the Entrust Bootloader should use when connecting to Cryptographic Security Platform Vault. By default, this dialog box shows the current DeviceID (a unique integer) and ConnectionID from `WMI class Win32_NetworkAdapter` for the selected network interface.
    c. When you are finished, click **Install**.
    d. If prompted, click **Yes** to remove any existing Bootloader partitions.
    e. The installer displays a prompt that the system is going to be upgraded and will require a reboot. Click **Yes** to continue with the upgrade.
    f. If this is the first time the Entrust Bootloader has been installed on this VM, after the machine has finished booting, copy the `id_rsa` key file to another location in case you ever need to access the Entrust Bootloader Debug Console using SSH. If you are upgrading an existing Bootloader installation, the `id_rsa` key file is not changed during the upgrade.

11 CSP Vault Appliance Management

Appliance Management is part of the Cryptographic Security Platform Vault Management webGUI. Click the Appliance Management link to switch views. When you are on the Appliance Management page, click the Manage Vaults link to return.

CSP Vault System Configuration

Enabling an HTTP Proxy Server in CSP Vault

If Cryptographic Security Platform Vault does not have direct access to the internet, you can configure an HTTP proxy server to use for BYOK.

> Note: The proxy settings affect the entire Cryptographic Security Platform Vault and also apply to all the vaults that you create.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Proxy Settings**.
5. On the Proxy Settings page, specify the following:
    - On the Basic tab, enter the IP/Hostname and the port number for the HTTP proxy server.
    - On the Advanced tab, optionally enter the username and password for the HTTP proxy server.

   Note: If your HTTP proxy server is configured without authorization, then you do not need to enter a username and password. We recommend that you use authentication.
6. When you are finished, click **Apply**.

Network Interface Configuration Options

When you install Cryptographic Security Platform Vault, you have to specify a valid network connection to make sure the Cryptographic Security Platform Vault node can communicate with other Cryptographic

Security Platform Vault nodes and with associated VMs. If your network changes or if you want to use multiple NICs (Network Interface Cards), you can update your settings using Manage Network Settings from the Entrust Cryptographic Security Platform Vault System Console on the node whose network settings you want to change.

The Manage Network Settings menu includes the following options:

Option	Description
Show Current Network Configuration	Lets you view the current network configuration for the node. If the node has multiple NICs, this option allows you to select which NIC configuration you want to view.
Manage IP Address Settings	Lets you change the current network configuration. If the node has multiple NICs, this option allows you to select which NIC configuration you want to change. For details, see Multi-NIC Node Configuration.
Disable a Network Interface	If the node is configured with multiple NICs, this option lets you remove one or more NICs from the configuration. For details, see Removing a NIC from the Configuration. Note: You cannot remove the management interface.
Manage DNS Settings	Lets you view and update your current DNS Settings. For details, see Configuring DNS Settings.
Manage NTP Settings	Lets you view and update your current NTP Settings. For details, see Configuring NTP Settings.
Manage Static Routes	Lets you add static routes for the Cryptographic Security Platform Vault node for environments where dynamic routing is not the optimal solution. For details, see Configuring Static Routes.
Network Diagnostic Tools	Lets you troubleshoot network issues. For details, see Troubleshooting Network Issues.

Multi-NIC Node Configuration

If you want to segregate the communication traffic across multiple channels, you can configure a Cryptographic Security Platform Vault node to use multiple virtual NICs (Network Interface Cards). For example, you may want one NIC to handle the communication between the Cryptographic Security Platform Vault webGUI and the Cryptographic Security Platform Vault nodes on `TCP/443` while a second NIC handles the cluster traffic and the internal node management traffic on `TCP/8443`. Multi-NIC configuration is only supported with the Cryptographic Security Platform Vault for Databases and the Cryptographic Security Platform Vault for VM Encryption for policy agent communication.

With multiple NICs, one NIC must be designated as the "management interface", and this interface must be able to communicate on port `TCP/8443`. Cryptographic Security Platform Vault uses the internal node management interface to:

- Determine the administrative MAC address for the node.
- Initializes the communication traffic between the nodes in the cluster.
- Handle any authentication requests that come into the cluster.

All management interface communication must take place on the management interface. You *cannot* split management communication across multiple interfaces.

Considerations

When you are configuring multiple NICs on a node, keep the following things in mind:

- Cryptographic Security Platform Vault supports a maximum of four virtual NICs. One NIC must be the management interface, as described above. In addition to the management interface, you can specify up to three additional NICs that can be used for inbound and outbound traffic. This includes inbound client and Cryptographic Security Platform Vault webGUI traffic as well as outbound syslog, NFS, and email traffic.
- All NICs must be of the same interface adapter type. For example, if the first NIC specified uses the adapter type VMXNET, all other NICs must be of type VMXNET.
- All NICs use global values for their DNS settings, NTP settings, default gateway, and DNS server list. Any change made to those settings on one NIC affects all NICs.
- When you deploy a new Cryptographic Security Platform Vault node through an OVA template or an ISO image, you must specify basic network information such as an IP address, domain, gateway, and DNS server list. When you do so, Cryptographic Security Platform Vault automatically designates that IP address as the management interface on port `TCP/8443`. We strongly recommend that you do not change this interface if the node is already part of a cluster or if any VMs have already been registered with the node.
  If you want to select the management interface during deployment, you must install Cryptographic Security Platform Vault from the ISO image on an existing VM that already has all of the required NICs configured. In this case, Cryptographic Security Platform Vault will prompt you to select the management interface during the installation.
- Adding additional NICs to the VM after deployment requires you to shut down the Cryptographic Security Platform Vault node while you add the NICs. You cannot add NICs to a running system.
  If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long. If the node is a standalone node, any VMs registered with the node will be unable to retrieve their keys while the network services are offline, and any VM heartbeats will fail.
- Cryptographic Security Platform Vault automatically restarts the network services on the node every time you change the configuration for a NIC. The node will be unavailable for a brief period until this process has finished.

Related Topics

- Configuring Multiple NICs on an Existing CSP Vault
- Removing a NIC from the Configuration

Configuring Multiple NICs on an Existing CSP Vault

When you deploy a new Cryptographic Security Platform Vault node, you configure the management interface during that process. We strongly recommend that you do not change this interface after you have deployed the node if the node is part of a cluster or if there are VMs registered with the node.

The following procedure describes how to add and configure additional NICs on an already-deployed node. For details about deploying a new Cryptographic Security Platform Vault node, see Installing CSP Vault from an OVA Template or Installing the First CSP Vault Node from an ISO Image.

Warning: During the following procedure, the node will be unavailable at certain points. If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long. If the node is a standalone node, any VMs registered with the node will be unable to retrieve their keys while the node is offline.

In addition, if the node is part of a cluster and you want to change the management interface, you must remove the node from the cluster first.

1. If the additional NICs you want to use have not yet been configured on the VM in which the Cryptographic Security Platform Vault node is running, do the following:
    a. If the Cryptographic Security Platform Vault node is powered on, shut it down using your hypervisor or the node's Entrust Cryptographic Security Platform Vault System Console. For details, see Using the Entrust CSP Vault System Console.
    b. In your hypervisor, add the new NICs to the Cryptographic Security Platform Vault VM and configure them using your corporate standards.
    Note: Make sure that the new NICs use the same adapter type as the existing NICs. For example, if the management interface NIC is of type VMXNET, the new NICs must be of type VMXNET as well.
    c. Make a note of the MAC address you are using for each NIC. When the NICs are displayed in Cryptographic Security Platform Vault, they are identified by their MAC address. Therefore, when you go to configure the NIC in Cryptographic Security Platform Vault later in this procedure, you will need to know its MAC address.
    d. Power on the Cryptographic Security Platform Vault VM.
2. Log in as `htadmin` on the Cryptographic Security Platform Vault node whose NICs you want to configure.
Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
3. Select **Manage Network Settings**.
4. Select **Manage IP Address Settings**.
5. On the **Interfaces** screen, select the NIC you want to configure and press **Enter**.
The NIC that is the current management interface has 'Current management interface' listed after the name. We strongly recommend that you do not change this interface after deployment if this node is part of a Cryptographic Security Platform Vault cluster or any VMs are registered with this node. If you select the management interface, acknowledge the configuration request at the prompt.
6. On the **Secondary Network Configuration** screen, specify the static IP address and netmask for the Cryptographic Security Platform Vault node.
Note:
    - Changing the hostname on one NIC changes it for all NICs, including the management interface NIC. If this node is part of a cluster, you should not change the hostname for the node.
    - All NICs must use the same default gateway and DNS server list.
    - Make sure you specify a static IP address and netmask for the Cryptographic Security Platform Vault node.
7. When you have finished specifying the network information, select **OK** and press **Enter**.
Cryptographic Security Platform Vault restarts the network services using the new configuration. Contact with the node via the Cryptographic Security Platform Vault webGUI or by any VMs registered with the node will be unavailable until the restart is finished.
When the network finishes restarting, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console.
8. Repeat the proceeding steps for any other NICs you want to configure. Cryptographic Security Platform Vault will restart the network services and the node will be unreachable for a short time after each configuration change.
9. If you want to verify the configuration information, select **Manage Network Settings**. From there, select **Show Current Network Configuration** to view a list of the configured NICs with their IP addresses and netmasks. The management interface IP address is shown as the main interface. Any additional interfaces that are configured are shown below.

Removing a NIC from the Configuration

If you want to remove a NIC that you have previously configured, you should use the Entrust Cryptographic Security Platform Vault System Console to disable that NIC in Cryptographic Security Platform Vault before you remove it from the VM.

In addition, if this node is part of a cluster we recommend that you remove it from the cluster before you remove the NIC. You can then re-join it with the cluster after the network configuration is complete.

Warning: This option is not reversible and it requires the node to reboot.

1. Log in as `htadmin` on the VM whose NIC you want to remove.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Network Settings**.
3. Select **Disable Network Configuration**.
4. Select the interface you want to disable.
   Note: You cannot disable the management interface, so Cryptographic Security Platform Vault does not show that interface in the list.
5. Confirm at the prompt.
6. Press **Enter** to reboot the node.
7. If desired, select **Shutdown System** and then use your hypervisor to remove the NIC from the VM.

Configuring DNS Settings

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage DNS Settings**.
3. On the **Modify DNS Settings** page, you can view your existing DNS settings. Select one of the following:
   - **No**—Exits the screen and returns to the Manage Network Settings page.
   - **Yes**—Opens the Network Configuration screen. Enter a comma-separated list of DNS addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the Manage Network Settings page.

Configuring NTP Settings

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage NTP Settings**.
3. On the **Modify NTP Network Settings** page, you can view your existing NTP settings. Select one of the following:
   - **No**—Exits the screen and returns to the Manage Network Settings page.
   - **Yes**—Opens the Network Configuration screen. Enter a comma-separated list of NTP addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the Manage Network Settings page.

Configuring Static Routes

In some network environments, it may be necessary to add static routes to Cryptographic Security Platform Vault rather than relying on dynamic routing.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage Static Routes**.
3. From the **Static Routes** page, you can:
    - View a list of the defined routes by selecting **List Current Static Routes**.
    - Add a new route by selecting **Add Static Route** and entering the route network address and gateway in the Add Static Route page. Cryptographic Security Platform Vault displays a message that the route has been successfully added.
    - Delete a previously-defined static route by selecting **Delete Static Route** and specifying the network address and gateway of the route you want to delete. Cryptographic Security Platform Vault displays a message that the route has been deleted.

Configuring TLS

Because each node hosts a standalone webserver, if you want to configure TLS for a node you must log into the webGUI for that specific node.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **TLS Configuration**.
5. On the **Protocol** tab, select the TLS authentication modes that you want to use:
    - TLSv1.2, TLSv1.3
    - TLSv1.3 only
6. Optionally, on the **Cipher Suite** tab, review the detailed list of available ciphers. If you want to remove ciphers from this list, click the **X** following the cipher name that you do not want to use. If you want to add a cipher, click in the bottom of the list box and enter a valid cipher name, then click **Reload**.
   The following ciphers are supported:
    - ECDHE-ECDSA-AES256-GCM-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
    - ECDHE-ECDSA-AES256-CCM
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-RSA-AES128-GCM-SHA256
    - ECDHE-ECDSA-AES128-CCM
    - DHE-RSA-AES256-GCM-SHA384
    - DHE-RSA-AES256-CCM
    - DHE-RSA-AES128-GCM-SHA256
    - DHE-RSA-AES128-CCM
    - PSK-AES256-GCM-SHA384
    - PSK-AES256-CCM
    - PSK-AES128-GCM-SHA256
    - PSK-AES128-CCM
    - DHE-PSK-AES256-GCM-SHA384
    - DHE-PSK-AES256-CCM

- DHE-PSK-AES128-GCM-SHA256
- DHE-PSK-AES128-CCM

7. On the **TLS Extended Master Secret** tab, select whether or not to enforce EMS. We highly recommend that you enable EMS.
   Important:
   - The EMS setting applies to the entire cluster. Changing the EMS will automatically reboot all nodes in the cluster. After rebooting, it may take the nodes several minutes to restart.
   - If you have EMS configured on your Cryptographic Security Platform Vault Appliance, you must disable it before you can connect to Cryptographic Security Platform Compliance Manager.
   - If you plan to use Double Key Encryption (DKE), TLS must be set to **TLSv1.2, TLSv1.3** and EMS must be set to **Do not enforce EMS**.
8. When you are finished, click **Apply**.

Uploading an OIDC CA Certificate

Because the Cryptographic Security Platform Vault certificate store is shared between the appliance and all individual vaults, if a vault using OIDC is locked out because the OIDC certificate expired, you can upload it here to restore access to the vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar click **Settings**.
4. In the General Settings section, click **OIDC CA Cert**.
5. On the OIDC CA Cert page, click **Load File** and locate the certificate that you want to upload.
   Note: Certificates must be in base 64 encoded .pem format.
6. Click **Upload**.

Setting Email Server Preferences

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Mail Server**.
4. On the **Mail** tab, specify the options you want to use.

Option	Description
Disable E-mail Notifications check box	If checked, no alert emails are sent to the user accounts in the system. If the Admin Key is regenerated, all security admins must manually download their key parts from the Settings tab. If this option is not selected, Cryptographic Security Platform Vault only sends alerts and new Admin Key parts through email. Security Admins can still download their Admin Key parts from the webGUI. For details about the Admin Key, see Admin Keys.

Option	Description
Server	The IP address or fully qualified domain name (FQDN) of the SMTP server. If your domain has an MX record configured, you can use Cryptographic Security Platform Vault to relay mail by setting the IP address to `127.0.0.1`. This is the default behavior.
Port	The mail server port.
Login	If required, the user account with which Cryptographic Security Platform Vault should log into the email server.
Password	The password for the login account.
Sender	The sender that Cryptographic Security Platform Vault should use when sending email.
SMTPS	If this option is set to On, Cryptographic Security Platform Vault uses SMTP Secure (SMTPS). Note: • If you disable SMTPS, and the server supports StartTLS, then when the connection is made StartTLS will be used. SMTPS is not compatible with StartTLS, and only one can be used. • Important information such as alerts and admin keys are shared by email. We highly recommend you set this option to use encryption with SMTP.

5. To test the email settings, click **Send Test Email**.

Setting CSP Vault Console Settings

If you do not remember the credentials of any user with the Security Administrator (`secroot`) privilege, or if you are locked out of the Cryptographic Security Platform Vault webGUI, Cryptographic Security Platform Vault provides a self-service option using the Cryptographic Security Platform Vault System Console to reset the `secroot`) user credentials with a temporary password. You can disable this option if you do not want this feature.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Console Settings**.
5. On the Cryptographic Security Platform Vault Console Settings page, select one of the following:
   - Select **YES** to allow the `htadmin` user to reset the `secroot` password.
   - Select **NO** if you do not want to allow the `htadmin` user to reset the `secroot` password.

6. Click **Apply**.

Syslog Server Settings

The Syslog Server Settings page allows you to view the settings of your Syslog Server, or enable or disable the server. When enabled, you can set the protocol to TCP or UDP, set the type of TLS authentication, the log format (RFC 5424 or CEF), and enter a list of syslog servers and their corresponding ports. You can also generate a certificate signing request, and, if required by your authentication mode, upload a CA certificate or client certificate. You can also reset the Syslog Server settings to the default values.

Configuring Syslog Server Settings

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Click the Switch to Appliance Management link at the top right.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Syslog Server**.
5. On the **Syslog Server Settings** page, specify the options you want to use.

Option	Description
State	Select ENABLED to use a syslog server.
Protocol	Select the protocol that you want to use. You can use TCP or UDP for syslog.
TLS Authentication List	Select one of the following: • No validation • x509/certvalid—Requires server certificate validation. • x509/name—Requires server certificate validation and hostname validation. • x509/fingerprint—Requires server certificate fingerprint. The fingerprint is a SHA1 hash of the server certificate, for example: "SHA1:00:11:22:33:44:55:66:77:88:99:00:11:22:33:44:55:66:77:88:99".
Server List	Enter the list of syslog servers and their corresponding ports. For the port, enter an outbound port between 25 and 65535.
Log Format	Select one of the following: • RFC 5424 • CEF
CA Certificate	Upload a CA certificate if you are using x509/certvalid or x509/name.

Option	Description
Client Certificate	Upload a client certificate if you are using x509/certvalid, x509/name, or x509/fingerprint.

6. Click **Apply**.

Important: If you plan to use an external syslog server for your audit logs, you must also complete the following:

1. Configure your syslog server to receive messages from each of the Cryptographic Security Platform Vault nodes in the cluster. The `syslogd` flags that specify the Cryptographic Security Platform Vault nodes should contain names that are resolvable. Make sure that your `/etc/hosts` file is set up correctly, with either IP addresses or hostnames. If you use hostnames, make sure that reverse lookups work on the syslog server.
2. Add the tag `hcs_audit` to your `syslog.conf` file. The FreeBSD example below directs all `hcs_audit` messages to go to the log file `/var/log/hcs_audit.log` :
   ```
   ! hcs_audit *.* /var/log/hcs_audit.log
   ! -hcs_audit
   ```
3. Make sure the audit log file is only writeable by `root` . For example:
   ```
   # touch /var/log/hcs_audit.log
   # chmod 0600 /var/log/hcs_audit.log
   ```
4. Configure your `rc.conf` file. For example, the following should be set prior to changing to `syslog.conf` :
   ```
   syslogd_enable="YES"
   syslogd_flags="-a kps1.domain -a kps2.domain -v"
   ```
5. Restart the syslog daemon and verify that audit records generated by every Cryptographic Security Platform Vault node are being written to the `hcs_audit.log` file by logging out and then log back in on each of the Cryptographic Security Platform Vault nodes in the cluster. When you are done, examine the audit log to make sure those logins were properly recorded.
   If messages are not being added, use **tcpdump** to make sure that packets are arriving at the syslog server. If the packets are arriving, check the documentation for your syslog server to make sure the configuration is correct.

Resetting Syslog Server Settings

You can reset the Syslog server settings to the default values.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, select **Syslog Server**.
5. Select **Actions > Reset to Default**.
6. At the prompt, select **Proceed**.

CSP Vault Certificates

- About CSP Vault Certificates
- Viewing the Expiration Date for the Current CSP Vault SSL Certificate

About CSP Vault Certificates

Cryptographic Security Platform Vault requires that an SSL certificate be installed on each Cryptographic Security Platform Vault node in a cluster. Each Cryptographic Security Platform Vault instance is installed with two web servers:

- An internal web server that manages the CSP Vault node to node cluster communication on port 8443.
- An external web server that manages the CSP Vault Web UI, the REST API interface, and the Policy agent communication on port 443.

By default, Cryptographic Security Platform Vault includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When the first Cryptographic Security Platform Vault node is installed, it creates a Private and Public CA that it also stores in the Cryptographic Security Platform Vault object store.

The first Cryptographic Security Platform Vault node then uses the Private CA to create an SSL certificate that contains the hostname (FQDN) as well as the IP address of the Cryptographic Security Platform Vault node for the internal web server and Public CA to create an SSL certificate that contains the hostname, both short and FQDN, as well as the IP address of the Cryptographic Security Platform Vault node for the external web server. When the node reboots, Cryptographic Security Platform Vault checks the IP address and recreates the SSL certificate if the IP address has changed.

Cryptographic Security Platform Vault node to node communication is on a TLS channel and it uses SSL certificates issued by Private CA to secure communication. When additional Cryptographic Security Platform Vault nodes are added to the cluster, the first Cryptographic Security Platform Vault node shares the Private and Public CA through the Cryptographic Security Platform Vault object store over an HTTPS connection.

In addition to creating an SSL certificate on each Cryptographic Security Platform Vault node, the Public CA also creates a matching CA certificate that is copied to a VM when the VM is registered with Cryptographic Security Platform Vault. The VM uses the CA certificate to verify Cryptographic Security Platform Vault's identity every time it receives a communication from Cryptographic Security Platform Vault. If the CA certificate on the VM cannot verify the SSL certificate that signed the communication, the VM rejects the communication.

The VM also has its own certificate that it uses to sign any communication it sends to Cryptographic Security Platform Vault. If Cryptographic Security Platform Vault determines that the VM's certificate is invalid or has expired, Cryptographic Security Platform Vault rejects the communication.

Because both the VM and Cryptographic Security Platform Vault verify any incoming communication, a "man in the middle" attack is not possible. The VM must be able to verify Cryptographic Security Platform Vault's identity and Cryptographic Security Platform Vault must be able to verify the VM's identity before any information is exchanged.

In this scenario, the Public CA installed on all the Cryptographic Security Platform Vault nodes is the same, ensuring that every Cryptographic Security Platform Vault node is able to verify SSL certificates generated by every other Cryptographic Security Platform Vault node in the cluster. However, this default SSL certificate is considered self-signed, which can lead to trust issues.

Cryptographic Security Platform Vault Certificate Options

You can replace the default SSL certificate configured on external and internal web server with an externally signed SSL certificate at any time by uploading the externally signed SSL certificate and its associated CA certificate to one of the Cryptographic Security Platform Vault nodes in the cluster.

If an externally signed SSL certificate is uploaded to be installed on internal web server, Cryptographic Security Platform Vault automatically distributes an updated CA certificate to all other nodes in the cluster.

If an externally signed SSL certificate is uploaded to be installed on external web server, Cryptographic Security Platform Vault automatically distributes an updated CA certificate to all registered VMs. The VMs can then use the updated CA certificate to validate any communication coming from Cryptographic Security Platform Vault. You can either use the same external SSL certificate on all Cryptographic Security Platform Vault nodes or you can use a different SSL certificate on each node. If you use different certificates, however, Entrust recommends that those certificates all be signed by the same certificate authority. For more information, see Installing External Certificates for Internal and External Webservers.

> Note: If you are generating an SSL certificate from openssl or other third-party tool, make sure you use a template designed for a web server certificate. Cryptographic Security Platform Vault registration may fail for some VMs if the SSL certificate is generated using a template designed for a Certificate Authority certificate.

You can also replace the current SSL certificate with a new self-signed certificate that will be automatically distributed to all Cryptographic Security Platform Vault nodes. If a new signed certificate is generated for external web server, Cryptographic Security Platform Vault does not need to communicate with the VMs because the default CA certificate is always copied to the VM during the registration process, even when Cryptographic Security Platform Vault is using an externally signed certificate. For more information, see Installing a New Self-Signed Certificate for a Node.

Viewing the Expiration Date for the Current CSP Vault SSL Certificate

It is critical to keep the Cryptographic Security Platform Vault certificate current. If it expires, Cryptographic Security Platform Vault will be unable to send keys to the registered VMs and data access will be denied until a valid certificate is installed.

Use the following procedure to view the expiration date for the current Cryptographic Security Platform Vault certificate on the selected Cryptographic Security Platform Vault node.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
5. To view the SSL certificate configured for the internal web server, click the link next to **Internal Web server** in the Certificate detail.
   The link name is **Default** if the internal web server is using the default self-signed certificate and **Custom** if it is using a custom SSL certificate.
6. To view the SSL certificate configured for the external web server, click the link next to **External Web server** in the Certificate detail.
   The link name is **Default** if the external web server is using the default self-signed certificate and **Custom** if it is using a custom SSL certificate.

7. When you are done, click **Close**.
8. If you want to check the expiration date for the certificate on another Cryptographic Security Platform Vault node, select that node and repeat this procedure.

Creating a Certificate Signing Request

A certificate signing request (CSR) tells an external Certificate Authority (CA) that you want an SSL certificate generated and signed by that CA. The SSL certificate can then be uploaded to Cryptographic Security Platform Vault and used in place of the default self-signed certificate.

When you use Cryptographic Security Platform Vault to create the CSR, Cryptographic Security Platform Vault creates a key pair and uses that key pair in conjunction with the information you specify to create the CSR. Cryptographic Security Platform Vault then encrypts the key pair and stores it for later use.

You can use the resulting CSR to generate an SSL certificate from the external CA you want to use. After you receive the SSL certificate from that external CA, you can upload it to Cryptographic Security Platform Vault. Because the key pair already exists on the system, you do not need to upload anything else.

If you create the CSR to generate an SSL certificate to be installed for internal web server, you must include the IP address of the Cryptographic Security Platform Vault node in Subject Alternative Name.

If you create the CSR outside of Cryptographic Security Platform Vault, you need to upload both the SSL certificate and the matching private key file when you install the certificate on Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
5. Select **Actions > Create CSR**.
6. In the Generate Certificate Signing Request dialog box, specify the options you want to use.

Field	Description
Common Name	The name to associate with this request. By default, Cryptographic Security Platform Vault enters the selected server name in this field. You can edit the default name as needed.
Locality	The locale to associate with this request.
State	The state to associate with this request.
Subject Alternative Names	The host names that will be protected by this certificate. If you want to use the same certificate on multiple Cryptographic Security Platform Vault nodes in the system for the external web server, add all of the Cryptographic Security Platform Vault URLs to this list. By default, Cryptographic Security Platform Vault adds the URL of the selected Cryptographic Security Platform Vault node. You can change or delete the default URL as long as you end up specifying at least one Cryptographic Security Platform Vault node in this field.

Field	Description
Key Size	Select the key size that you want to use. The default is 4096 bytes.
Country	The ISO 3166-1 alpha-2 code of country to associate with this request. The default is US.
Organization	The organization to associate with this request.
Organization Unit	The organizational unit associate with this request.

7. Click **Generate**.
8. When you receive the message that Cryptographic Security Platform Vault has created the CSR, click **Download** to save a copy of the CSR to your browser's default download directory or click **Preview** to view the CSR in a pop-up window. You can copy the CSR from the Preview window to the clipboard if desired.
9. Use the CSR to request an SSL certificate from the external Certificate Authority you want to use. How you do this depends on the CA you are using.

What to Do Next

After you receive the SSL certificate from the external CA, install it on Cryptographic Security Platform Vault as described in Installing External Certificates for Internal and External Webservers.

Using Self-Signed Certificates for All Nodes in a Cluster

If you plan to use self-signed certificates, we recommend that you use them for all nodes in the cluster. You can now set the entire cluster to accept self-signed certificates.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Cluster** tab and select **Actions > Use Self-Signed Certificate**.
5. Click **Proceed** at the prompt.
   Cryptographic Security Platform Vault generates a new self-signed certificate for all nodes in the cluster, and then restarts the server. You will need to log back into Cryptographic Security Platform Vault after the restart.
   Tip: If you are using IE, you may receive an alert stating that revocation information for the certificate is not available. Click **Yes** to acknowledge the alert and restart the web service. If you are using Chrome and you receive a series of connection errors when the web service restarts, open the webGUI login page in a new tab.
   To view the certificates, click the Servers tab, select a node, and then click the links next to **Internal/ External web server**.

Generating and Installing a Custom Self-Signed Certificate

Use this procedure to generate and install a custom self-signed certificate for all nodes in your cluster. If you are using a KMIP server you can choose to use this certificate for the KMIP server as well.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Cluster** tab and select **Actions > Generate and Install Self-Signed Certificate**.
5. Complete the following:

Field	Description
Common Name	The name to associate with this certificate. This field is required.
Locality	Optional. The locale to associate with this certificate.
State	Optional. The state to associate with this certificate.
Subject Alternative Names	Optional. The host names that will be protected by this certificate. If you want to use the same certificate on multiple Cryptographic Security Platform Vault nodes in the system for the external web server, add all of the Cryptographic Security Platform Vault URLs to this list. By default, Cryptographic Security Platform Vault adds the URL of the selected Cryptographic Security Platform Vault node. You can change or delete the default URL as long as you end up specifying at least one Cryptographic Security Platform Vault node in this field.
Key Size	Optional. Select the key size that you want to use. The default is 4096 bytes.
Country	The ISO 3166-1 alpha-2 code of country to associate with this certificate. This field is required.
Organization	Optional. The organization to associate with this request.
Organization Unit	Optional. The organizational unit associate with this request.
Validity (Days)	Optional. The number of days this certificate will be valid. The default is 365 days.
Use this certificate for KMIP	Select Yes if you are using a KMIP server along with the Cryptographic Security Platform Vault for KMIP and want to use this certificate for the KMIP server as well. The default is No.

6. Click **Generate and Install**.

Installing External Certificates for Internal and External Webservers

Use this procedure to replace the current Cryptographic Security Platform Vault SSL certificate with a new externally-signed SSL certificate. If you want to use a new, self-signed SSL certificate generated by the Public CA or Private CA included with Cryptographic Security Platform Vault, see Installing a New Self-Signed Certificate for a Node.

Before You Begin

- If you generated external certificates using Microsoft Active Directory Certificate Services, then the certificates will be in .p7b format. Because Cryptographic Security Platform Vault only accepts certificates in base64-encoded PEM format, you will need to convert the file using the following:
    a. Run `openssl pkcs7 -in cert.p7b -inform p7b -print_certs -out cert.pem`, where cert.p7b is the input certificate in .p7b format and cert.pem is the converted certificate in .pem format.
    b. If you have a certificate chain with no separate server certificate and CA certificate/chain, the first certificate in the chain is generally used as the server certificate, and all other certificates would be the CA certificate chain. In this case, you can break up the chain into two files, with server.pem containing the server certificate (the first certificate) and cacert.pem containing the remaining certificates.
    If this occurs, verify that the separation is correct by running `openssl verify -verbose -CAfile server.pem cacert.pem`, where server.pem is the server certificate and and cacert.pem are is the CA certificate/chain.
- If you generated the Certificate Signing Request (CSR) through Cryptographic Security Platform Vault, you need to make sure you have the resulting SSL certificate and the CA certificate in Base64-encoded pem format files accessible to the Cryptographic Security Platform Vault node that you are logged into. If you generated the CSR through some other means, make sure you have both of the Base64-encoded pem format certificates and the Base64-encoded pem format private key file that goes with the certificates. Cryptographic Security Platform Vault supports only RSA private keys. For more information, see Creating a Certificate Signing Request.
- If you generated the SSL certificate from openssl or other third-party tool, make sure the certificate is formatted as a web server certificate. Cryptographic Security Platform Vault registration may fail for some VMs if the SSL certificate is formatted as a Certificate Authority certificate.
- The SSL certificate generated for the internal web server should be able to function as the Client and Server certificate.
- SSL certificates that contain an intermediate CA certificate chain are not supported for the internal web server. If there is a certificate chain, it must be specified in the CA certificate for the internal web server.
- We strongly recommend that you verify all VMs registered with Cryptographic Security Platform Vault are online and accessible before you install a new SSL certificate on Cryptographic Security Platform Vault for the external web server. During the installation process, Cryptographic Security Platform Vault sends an updated version of the CA certificate to each of the registered VMs at their next heartbeat. If all VMs are online, this process is fairly simple and ensures that there is no interruption in the communication between the VMs and Cryptographic Security Platform Vault. If any VMs are inaccessible, however, the CA certificate may need to be manually updated on those VMs after the SSL certificate installation on Cryptographic Security Platform Vault is complete because the old CA certificate installed on the VMs will no longer be able to verify Cryptographic Security Platform Vault's identity and all communication coming from Cryptographic Security Platform Vault will be rejected by the VMs.
- Externally signed custom certificates must have the "Key Usage" extension set to "Digital Signature" and "Key Encipherment".

Procedure

1. Sign in to the Cryptographic Security Platform Vault Management webGUI with domain admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.

Note: You can use SSL certificates signed by different certificate authorities on individual Cryptographic Security Platform Vault nodes. However, Entrust recommends that all of the SSL certificates be signed by the same Certificate Authority so that only one CA certificate is required on the VMs registered with Cryptographic Security Platform Vault.

4. Select **Actions > Install Certificate**.
5. In the **Certificate** tab of the Certificate Installation dialog box, specify the options you want to use.

Field	Description
SSL Certificate	The SSL certificate file in Base64-encoded pem format. This certificate must be valid for the installation to succeed.
CA Certificate	The certificate of the CA that issued the SSL certificate in Base64-encoded pem format. The VMs registered with Cryptographic Security Platform Vault use the CA certificate to verify communication with Cryptographic Security Platform Vault.
Web Server	Choose which web server (External for port 443 or Internal for Port 8443) to install the custom certificate. You can select both if you wish to install the same SSL certificate for the internal and the external web server. If the SSL certificate is used for both web servers, it should be able to function as a Client and Server certificate and it should have the Cryptographic Security Platform Vault IP address specified in SAN.

Important: Before Cryptographic Security Platform Vault installs the certificate, it checks with the certificate authority to make sure that the SSL certificate can be validated.
If using a CA Certificate Chain, where the Server Certificate is signed by Intermediate CA, Entrust recommends:

- The Server Certificate (SSL Certificate) should be a separate SSL Certificate file.
- The CA Certificate of the intermediate CA and its chain leading to self-signed root CA certificate should be in a single CA certificate file and arranged as shown below:

```
-----BEGIN CERTIFICATE-----
Intermediate CA Certificate that signed Server Certificate
-----END CERTIFICATE-----
.
.
. there can be a chain of intermediate CA certificates here
.
.
-----BEGIN CERTIFICATE-----
Root CA Certificate signed by itself (self-signed root CA Certificate)
-----END CERTIFICATE-----
```

Ensure the Server has a purpose set. You configure this using the External Key Usage property of the Server Certificate accordingly.
a. If using the certificate for External Web Server, Server Authentication must be enabled.
b. If using the certificate for Internal Web Server, both Server & Client Authentication must be enabled.

This would be `extendedKeyUsage = serverAuth, clientAuth` in openssl.cnf (OpenSSL config) of the Certificate Authority issuing Server Certificate. It can be verified by running `openssl x509 -purpose -noout -in server.pem` on the server Certificate. as shown in the example below:

```
# openssl x509 -purpose -noout -in server.pem
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : Yes
S/MIME signing CA : No
S/MIME encryption : Yes
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
```

`SSL server : Yes` (line 5) indicates Server authentication is enabled. `SSL client : Yes` (line 3) indicates Client authentication is enabled.

6. If you did *not* create the certificate signing request with Cryptographic Security Platform Vault:
    a. Click the **Private Key** tab and click **Load File**, then navigate to the private key file you want to use. Cryptographic Security Platform Vault never stores the private key in clear text.
    b. If the private key file is encrypted, enter the user-specified password for the key file in the **Password** field. This password is not stored in the Cryptographic Security Platform Vault object store or on the local file system.
7. Click **Install Certificate**.
   If an SSL certificate is to be installed for the external web server and if there are any VMs already registered with the system, Cryptographic Security Platform Vault automatically distributes the new CA certificate to those VMs on their next heartbeat and tracks the progress of the install in the **Certificate State** field. Cryptographic Security Platform Vault updates the installation status shown in the webGUI every 5 minutes. The state can be:
    - IN PROGRESS—The install is in progress. The table displays one line for each Cryptographic Security Platform Vault node showing the total number of VMs, the number of VMs that timed out and could not be reached, and the number that are waiting for the web service to restart.
      If a new VM is added to Cryptographic Security Platform Vault or a previously-inaccessible VM comes back online during this phase, Cryptographic Security Platform Vault automatically sends the appropriate CA certificate to that VM as soon as there is a successful VM heartbeat.
      The length of time this phase takes depends on heartbeat duration configured for the registered VMs and whether all of those VMs are accessible. Cryptographic Security Platform Vault polls for responses once every 5 minutes. If all VMs have had a successful heartbeat during that time, Cryptographic Security Platform Vault completes this phase and changes the installation status to RESTART PENDING. If one or more VMs have not yet been contacted or if their heartbeat has failed, Cryptographic Security Platform Vault waits another 5 minutes and polls again.
      This process continues until all registered VMs have either been successfully contacted or have failed 4 consecutive heartbeats. If even one VM is inaccessible, the entire installation process remains in this phase until that VM either comes back online or has failed the fourth scheduled heartbeat. In the latter case, Cryptographic Security Platform Vault considers the installation request to have timed out for that VM and it sets the installation status to TIMED OUT.
      For example, If you are using the default heartbeat duration of 5 minutes, that means Cryptographic Security Platform Vault will wait at least 20 minutes until it considers the request to have timed out. If you have increased the heartbeat duration for any of the VMs registered with Cryptographic Security Platform Vault, then this step will take longer. If you have increased the heartbeat for a particular VM to 1 day, Cryptographic Security Platform Vault may have to wait up to 24 hours before the next scheduled VM heartbeat occurs and it can update the status of the installation request to RESTART PENDING. If that VM is inaccessible, Cryptographic Security Platform Vault has to wait for 4 days before it stops trying to update that VM. It is only when the last VM has been contacted or has timed out that Cryptographic Security Platform Vault concludes this phase.
      Tip: If you do not want to wait for the next scheduled heartbeat on a particular VM, log into that VM as an administrator and issue the `hcl heartbeat` command on that VM. This allows Cryptographic Security Platform Vault to update the certificate information on the VM immediately.
    - RESTART PENDING—The install is completed and the new certificate will be used as soon as the web service is restarted. Cryptographic Security Platform Vault has successfully sent the new CA certificate to all registered VMs, so there should be no interruption in service once the web service restarts.
    - TIMED OUT—At least one of the VMs associated with the Cryptographic Security Platform Vault node could not be reached and the new CA certificate could not be sent to those VMs. When a VM times out, Cryptographic Security Platform Vault sends an alert to the Cloud Admins associated with that VM. The Cloud Admins are responsible for updating the Cryptographic Security Platform Vault CA certificate on the unreachable VMs. For more information, see Troubleshooting Certificate Issues.

8. If you install the SSL certificate for the internal web server, the web server automatically restarts.
   If you install the SSL certificate for the external web server, when the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service** and confirm the request at the prompt.
   After the web service restarts, Cryptographic Security Platform Vault will use the new certificate.
   Cryptographic Security Platform Vault restarts the web server which may interrupt the browser connection to the webGUI. When the restart is finished you are returned to the webGUI login page.
   Tip: If you are using Chrome, the connection status in your browser may still show as insecure. To fix this, open the Cryptographic Security Platform Vault Management webGUI login page in a new tab.
9. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.
   If you already have a custom certificate installed for external web server and the Cryptographic Security Platform Vault internal web server uses a default self signed SSL certificate, Cryptographic Security Platform Vault automatically detects and provides an option to use the same custom SSL certificate for internal web server if it meets the certificate requirements of the internal web server. Select **Use external Web server SSL certificate for internal Web server** and click **Save** to install the same custom SSL certificate for the internal web server.
   If you already have a custom certificate installed for the internal web server and the Cryptographic Security Platform Vault external web server uses a default self signed SSL certificate, Cryptographic Security Platform Vault automatically detects it and provides an option to use the same custom SSL certificate for the external web server if it meets the certificate requirements of the external web server. Select **Use internal Web server SSL certificate for external Web server** and click **Save** to install the same custom SSL certificate for internal web server. When the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service**, then confirm the request at the prompt. After the web service restarts, Cryptographic Security Platform Vault will use the custom SSL certificate for external web server.
   You can also use the `openssl verify` command to ensure that you are using the correct server certificate and CA certificate combination:

```
$ openssl verify -verbose -CAfile cacert.pem server.crt
server.crt: OK
```

CSP Vault Certificate Expiration Notification

Cryptographic Security Platform Vault checks internal and external web server certificates for expiration starting 21 days before the expiration date. The alerts are sent once per day until the certificate is replaced.

- If email notification is enabled, you will receive alert notifications by email.
- In the audit log, you will see alerts for the following:
  - 249 - External web server certificate has expired.
- 250 - External web server certificate will expire within x amount of time in days and hours.
- 467 - Internal web server certificate has expired.
- 468 - Internal web server certificate will expire within x amount of time in days and hours.

Installing a New Self-Signed Certificate for a Node

Use this procedure to replace the current Cryptographic Security Platform Vault certificate on configured on an internal or external web server with a new self-signed certificate generated by the certificate authority that is included with Cryptographic Security Platform Vault.

Note:

- This procedure is for an individual node only.
- If you want to install an externally-signed SSL certificate from a Base64-encoded pem format file, see Installing External Certificates for Internal and External Webservers.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
   Note: You can use a different certificate on each Cryptographic Security Platform Vault node. In this case, however, Entrust recommends that all of the certificates be signed by the same Certificate Authority.
5. Select **Actions > Use Self-Signed Certificate**.
6. Select the web server on which the self-signed certificate is to be installed.
7. Click **Proceed** at the prompt.
   If you select the external web server, CSP Vault restarts the web server. This may interrupt the browser connection to the webGUI. When the restart is finished, you are returned to the webGUI login page.
   Tip: If you are using IE, you may receive an alert stating that revocation information for the certificate is not available. Click **Yes** to acknowledge the alert and restart the web service. If you are using Chrome and you receive a series of connection errors when the web service restarts, open the webGUI login page in a new tab.
8. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.

Downloading a CSP Vault CA Certificate

You may need to download the CA certificate that can verify Cryptographic Security Platform Vault's SSL certificate and upload it to a VM if that VM was inaccessible when the Cryptographic Security Platform Vault SSL certificate was updated.

Warning: Do not rename the downloaded certificate. The name of the certificate has additional information and a renamed certificate will fail.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. Select **? > Download CA Certificate**.

The CSP Vault downloads a `pem` file to your browser's default download location.

Troubleshooting Certificate Issues

When you install a new, externally-signed SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the CA certificate on all registered VMs at their next heartbeat.

If any of the VMs are unreachable for 4 consecutive heartbeats, Cryptographic Security Platform Vault considers the update request to have timed out for those VMs. It sends one alert for each inaccessible VM to the Cloud Admins associated with that VM and then continues with the SSL certificate installation process.

The next time one of the inaccessible VMs boots, it may be unable to retrieve the proper keys from Cryptographic Security Platform Vault because the old CA certificate the VM is using cannot verify the new Cryptographic Security Platform Vault SSL certificate. The VM will then reject any communication from Cryptographic Security Platform Vault until it has the correct CA certificate installed and can once again verify Cryptographic Security Platform Vault's identity.

If there are encrypted data drives on the VM, Cryptographic Security Platform Vault will not attach those drives when the VM reboots. If the boot partition is encrypted on the VM, the VM will fail to boot. At this

point you need to manually update the CA certificate on the VM in order to restore the communication between the VM and Cryptographic Security Platform Vault.

For more information, see:

- Manually Updating the CA Certificate on a Data Encrypted VM. After you update the CA certificate, the VM can retrieve the keys from Cryptographic Security Platform Vault and the encrypted drives will be automatically reattached.
- Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM.
- Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM.

Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a Linux root-drive-encrypted VM was inaccessible during this process, that VM may not be able to boot because the CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

Important: Manually updating the certificate requires `ssh` access to the VM. If you did not enable the Entrust Debug Console when you ran the `htroot encrypt` command on the root drive, you need to contact Entrust Support at hytrust.support@entrust.com.

The following procedure is for Linux VMs with an encrypted root drive. For other types of VMs, see Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM or Manually Updating the CA Certificate on a Data Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.
2. Download the Bootloader SSH key for the VM so that you can open an SSH session and copy the new certificate file to the Bootloader:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
   b. Navigate to the **Workloads > VMs** tab and select the VM whose CA certificate you want to update.
   c. Select **Actions > Download Bootloader SSH Key**. The Cryptographic Security Platform Vault for VM Encryption downloads the SSH key to file called `server-name.key` in your browser's default download location. For example, if the server name is rhelsvr74, the SSH key file would be called `rhelsvr74.key` .

3. Open an `ssh` session and access the Entrust Debug Console on the root drive encrypted VM by entering the command `ssh -i server-name.key root@vm_name`, where `server-name.key` is the name of the SSH key file and `vm_name` is the IP address or hostname. For example:
   # ssh -i ~/Downloads/rhelsvr74.key root@192.168.140.133
   Warning: Permanently added '192.168.140.133' (RSA) to the list of known hosts.
   BusyBox v1.20.2 (Ubuntu 1:1.20.0-8.1ubuntu1) built-in shell (ash)
   Enter 'help' for a list of built-in commands.

   HyTrust Debug Console

   1. Show HT encryption log file
   2. Authenticate
   3. Show Network info
   4. Restart Network
   5. Advanced access
   6. logout

   Action:
4. Select `Advanced access`. The Entrust Policy Agent displays a secure shell prompt (sh). For example:
   Action: 5
   sh-10.5.3#
5. Open a second `ssh` session and copy the CA certificate file to the VM by entering the command `scp -i server-name.key cacert.pem root@vm_name:cacert.pem`, where `server-name.key` is the name of the SSH key file, `cacert.pem` is the fully qualified path to the pem file, and `vm_name` is the IP address or hostname. For example:
   $ scp -i ~/Downloads/rhelsvr74.key ~/Downloads/180412071755_cacert.pem root@192.168.140.133:180412071755_cacert.pem
6. Return to the Entrust Debug Console on the encrypted VM and update the certificate by entering the command `hcl update_ca -f cacert.pem`, where `cacert.pem` is the fully qualified path to the pem file. For example:
   sh-10.5.3# hcl update_ca -f ./180412071755_cacert.pem

   Updating using cert file at: ./180412071755_cacert.pem
   Updated CA certificate
7. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
8. Enter the command `hcl status` to confirm that the last heartbeat between the VM and Cryptographic Security Platform Vault was successful. For example:
   sh-10.5.3# hcl heartbeat
   sh-10.5.3# hcl status

   Summary

   KeyControl: 10.238.65.65:443
   KeyControl list: 10.238.65.65:443 10.238.65.66:443
   KeyControl Mapping: kc41-nodes
   Status: Reauth needed (Virtual Machine not authenticated)
   Last heartbeat: Tue Oct 24 22:19:32 2017 (failed)

AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT

9. If the `hcl status` command says that the VM needs to be re-authenticated, enter the command `hcl auth -a [-u user [-s password]]` , where:
   - `-u` is a Cryptographic Security Platform Vault user account name with Cloud Admin privileges.
   - `-p` is the password for the Cloud Admin account.

   If you do not provide a user name and password, you will be prompted for one. For example:
   sh-10.5.3# hcl auth -a
   Please provide the KeyControl login details
   username: secroot
   password:
   Completing authentication on KeyControl node

   Authentication complete, machine ready to use
10. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
11. If the heartbeat is successful, enter the command `exit` to leave the secure shell and select `logout` from the Entrust Debug Console main menu. The VM should automatically continue booting from the encrypted root drive.

Manually Updating the CA Certificate on a Data Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a data-drive encrypted VM was inaccessible during this process, the encrypted drives may become inaccessible because the CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

The following procedure is for VMs with encrypted data drives only. For other types of VMs, see Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM or Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from the Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.

2. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
3. Copy the Cryptographic Security Platform Vault for VM Encryption CA certificate `pem` file to the VM.
4. Enter the command `hcl update_ca -f /path/to/cert.pem`, where `/path/to/cert.pem` is the path to the CA certificate file.
   ```
   # hcl update_ca -f /etc/ssl/certs/171012172410_cacert.pem

   Updating using cert file at: 171012172410_cacert.pem
   Updated CA certificate
   ```
5. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
6. Enter the command `hcl status` to confirm that the last heartbeat between the VM and Cryptographic Security Platform Vault was successful.

Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a Windows boot-drive-encrypted VM was inaccessible during this process, that VM may not be able to boot because the CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

The following procedure is for Windows VMs with an encrypted boot drive. For other types of VMs, see Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM or Manually Updating the CA Certificate on a Data Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from the Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.
2. If needed, reboot the VM and wait for the Console menu to appear.
   If you are unable to view the console directly, for example in environments such as Amazon Web Services (AWS), you can access the console using an SSH client. This requires the `id_rsa` key file generated during the Policy Agent installation. Copy the `id_rsa` file to the server an then reboot.

   Tip: If you need another copy of the `id_rsa` key file, you can download it from the Cryptographic Security Platform Vault webGUI by selecting the VM on the **Cloud > VMs** tab and then selecting **Actions > Download Bootloader SSH Key**.

3. From the Console menu, select **Drop to shell**.
4. Copy the Cryptographic Security Platform Vault for VM Encryption certificate `pem` file to the VM.
5. Enter the command `hcl update_ca -f /path/to/cert.pem`, where `/path/to/cert.pem` is the path to the certificate file.
   ```
   # hcl update_ca -f /etc/ssl/certs/171012172410_cacert.pem

   Updating using cert file at: 171012172410_cacert.pem
   Updated CA certificate
   ```
6. After the certificate is successfully updated, enter the command `touch /opt/hcs/etc/updatecert` to tell the hcl service that the certificate has changed. The hcl service then syncs the change from the Bootloader back to the client installation directory.
   ```
   # touch /opt/hcs/etc/updatecert
   ```
7. Enter the command `exit` to leave the secure shell.
8. Select `Boot Windows with encryption key`. Cryptographic Security Platform Vault reboots the VM using the updated Cryptographic Security Platform Vault certificate.
9. If the VM reboots but displays an error that it needs to be authenticated, select **Reauthenticate** from the Console menu.
10. To verify that the VM is connected to Cryptographic Security Platform Vault:
    a. Open a Command Prompt on the VM.
    b. Enter `hcl heartbeat` to force the VM to communicate with Cryptographic Security Platform Vault and update the connection status.
    c. Enter `hcl status` to verify the connection status.

    ```
    C:\users\administrator> hcl heartbeat
    C:\users\administrator> hcl status

    Summary
    ----------------------------------------------------------------------------
    KeyControl: 10.238.65.65:443
    KeyControl list: 10.238.65.65:443 10.238.65.66:443
    KeyControl Mapping: kc41-nodes
    Status: Connected
    Last heartbeat: Tue Oct 24 22:30:32 2017 (successful)
    AES_NI: enabled
    Certificate Expiration: Sep 11 22:16:13 2020 GMT
    ```

Admin Keys

All Cryptographic Security Platform Vault data (policy information, encryption keys, user account information, and so on) are held in an encrypted object store that is shared across all Cryptographic Security Platform Vault nodes in the cluster.

The object store is ultimately protected (through multiple layers of key wrappings) by an Admin Key that Cryptographic Security Platform Vault generates and maintains. This key is required if you ever need to restore Cryptographic Security Platform Vault from a backup or you need to change the hardware configuration of a Cryptographic Security Platform Vault node. The Admin Key is a 4096 bit RSA asymmetric key pair.

When you install the first Cryptographic Security Platform Vault node in your system, Cryptographic Security Platform Vault generates an Admin Key as soon as you log into the Cryptographic Security Platform Vault Management webGUI for the first time. The initial key has a single part and is assigned to the

default `secroot` user account. As you add additional Security Administrator accounts to the system, Cryptographic Security Platform Vault shifts to an "n of m" Admin Key backup model, where "m" is the number of user accounts with Security Admin privileges and "n" is a user-defined value that states how many key parts must be uploaded before Cryptographic Security Platform Vault considers the Admin Key to be valid.

For example, if you have five Security Admins and you set n to 3, then at least three of the Security Admins will need to upload their Admin Key parts in order to restore Cryptographic Security Platform Vault from a backup. If you set n to 1, then any one of the five Security Admins can restore Cryptographic Security Platform Vault without consulting with any of the other Security Admins.

While you can regenerate Admin Key parts at any time, in order to restore Cryptographic Security Platform Vault from a backup image you must have the required number of Admin Key parts that were valid when the backup was created. You cannot regenerate the Admin Key parts and then immediately use those new key parts to restore Cryptographic Security Platform Vault from a previously-created back up.

The Admin Key is assigned a generation count that is incremented each time a new Admin Key is generated. This generation count allows you to identify which Admin Key parts go together. The email that each Security Admin receives when a new Admin Key is generated contains the generation count. For example:

> This current Key Part supersedes any you may have previously received from this cluster. The Key Part is associated by a "generation count" with its relevant backups. The generation count for this key is:
>
> 8

The generation count is also included in the Admin Key Part filename, which is attached to the email. The attachment name is *username_kc-ip-addr*.key.gen# , where `username` is the Security Admin's Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address from which the Admin Key was generated, and `#` is the generation count. For example, `secroot_10.238.66.235.key.gen8` . This same naming convention is used if a Security Admin downloads their Admin Key Part from the Cryptographic Security Platform Vault Management webGUI.

If you want to restore Cryptographic Security Platform Vault from a backup created when the Admin Key shown above was valid, you must make sure that all the Admin Key Parts you upload have generation count = 8.

External Admin Key Storage

You can store the entire Admin Key on an external key server (EKS), such as a Hardware Security Module (HSM). If you configure an EKS, you can restore the Admin Key using the entire key from the EKS.

This has the advantage that Security Admins do not need to worry about which Admin Key parts are required for which backup image. Cryptographic Security Platform Vault automatically fetches the appropriate key from the EKS and no manual synchronization is needed.

If you configure one or more EKS, Cryptographic Security Platform Vault stores the Admin Key on each EKS automatically and you can restore the Admin Key from any configured EKS. If an EKS is configured, administrators do not define the storage location and Admin Key parts are no longer available for download.

For details about using an EKS, see Hardware Security Modules with CSP Vault.

- Downloading Your Admin Key Part
- Generating the Admin Key
- Verifying the Admin Key

Downloading Your Admin Key Part

Every user account with Security Admin privileges receives an encrypted Admin Key part.
Certain Cryptographic Security Platform Vault functions, such as restoring the system from a backup, require that a certain number of parts be uploaded to Cryptographic Security Platform Vault within a certain amount of time. Once Cryptographic Security Platform Vault receives the correct number of parts, it can validate the Admin Key and perform the requested procedure. Once you download your key part, make sure you store it securely and that you can find it when needed.

> Note: If an external key server (EKS) is used to store Admin Keys, administrators do not define the storage location and Admin Key parts are no longer available for download. For more information, see Admin Keys.

Important: You also need to keep previous Admin Key parts and know when each part was created. If you need to restore a system from a previous backup, you must have the key parts that were valid when that backup was created. If the Admin keys have been regenerated, you cannot download the current Admin Key parts and use those to restore a previous version of Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Account Settings** section, click **Download Key**. Cryptographic Security Platform Vault downloads a file to your browser's default download location called *username_kc-ip-addr*.key.gen# , where `username` is the currently logged in Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address into which you are currently logged in, and `#` is the generation count. For example, secroot_10.238.66.235.key.gen8 .
5. If you want to remove the Admin Key part from the Cryptographic Security Platform Vault encrypted object store, click **Clear Key**. If you later attempt to download the key part after clearing it, you will get an error stating that the key part does not exist. You will need to regenerate the key as described in Generating the Admin Key.

Generating the Admin Key

When Cryptographic Security Platform Vault generates an Admin Key, it cryptographically divides the key into parts and sends one part to each Cryptographic Security Platform Vault user account with Security Admin privileges. In addition, if you have specified an EKS (external key server), Cryptographic Security Platform Vault stores a copy of the entire Admin Key on the EKS.

Cryptographic Security Platform Vault automatically generates new Admin Key:

- During installation of the first Cryptographic Security Platform Vault node. In this case, the **secroot** user account gets an Admin Key with a single part.
- When a Security Admin user account is added or deleted. In this case, a new Admin Key is divided into a new number of parts, "m", and sent to all current Security Admins.
  Note: The value of "n" is not changed. If you add three Security Admins immediately after the initial installation, the Admin Key will be divided into four parts, but only one part will be required when restoring the system. The way you set the required number of parts is described below.
- When you first configure Cryptographic Security Platform Vault to use an EKS.
- When you explicitly generate new a new Admin Key, as described below. In this case, the number of Admin Key parts is not changed.

> Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.

Note: If an external key server (EKS) is used to store Admin Keys, administrators do not define the storage location and Admin Key parts are no longer available for download. For more information, see Admin Keys.

Before You Begin

If you have configured Cryptographic Security Platform Vault to store the Admin Key in an external KMIP server or HSM (hardware security module), make sure that KMIP server or HSM is available before you generate a new Admin Key. If Cryptographic Security Platform Vault cannot store the Admin Key on the external device, the generate request will fail.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges. In the top right, click the Switch to **Appliance Management** link.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Admin Key Parts**.
4. Verify the following options:

Option	Description
Minimum Key Parts	The minimum number of parts needed when you want to restore Cryptographic Security Platform Vault from a back up ("n") and you are not retrieving the key from an EKS.
Email Private Key on Generate	If Enabled, when you generate a new Admin Key, Cryptographic Security Platform Vault automatically sends each Security Admin their key part as an email attachment. The attachment name is *username_kc-ip-addr*.key.gen# , where `username` is the Security Admin's Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address into which you are currently logged in, and `#` is the generation count. For example, secroot_10.238.66.235.key.gen8 . If Disabled, when you generate a new Admin Key, Cryptographic Security Platform Vault sends each Security Admin an alert stating that the admin key has been changed and prompting them to download their key part.

5. Click **Generate New Key**. Cryptographic Security Platform Vault increases the generation count by one and creates a new key part for each Security Admin in the system. If you have configured an EKS, Cryptographic Security Platform Vault also saves the Admin key to the EKS.
   Based on the setting of the **Email Private Key on Generate** option, Cryptographic Security Platform Vault also sends each Security Admin in the system an email with their key part or an alert stating that there is a new key part ready for download.
   Tip: If you intend to back up Cryptographic Security Platform Vault in the immediate future, we recommend that you notify your Security Admins that the new Admin Key part they just received is going to be tied to a backup image and they should download it to a secure location immediately. You cannot restore Cryptographic Security Platform Vault from a backup image unless you have the Admin Key parts that were valid when the back up was created, and you cannot download previous Admin Key parts from Cryptographic Security Platform Vault.
6. Click **Close**.

Verifying the Admin Key

Every 90 days, Cryptographic Security Platform Vault checks to ensure that the admin key you downloaded is still accessible. The Recovery Verification Required dialog box is displayed to prompt you to enter the admin key or regenerate it. If you close the window without verifying or regenerating the key, the dialog will be shown again the next time you log in.

Important: If the Admin Key is stored in EKS (HSM) then Cryptographic Security Platform Vault does not perform this check.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the General Settings section, click **Admin Key Parts**.
5. In the Admin Key Parts window, click **Verify Current Key**.
6. In the Recovery Verification Required page, click **Browse** to select your current Admin Key, and then click **Verify**.
   Note: If you do not have the Admin key, you can generate another one. See Generating the Admin Key.

If successful, the page will display the following message: Admin key is successfully verified. This dialog will then be repeated after another 90 days.

KMIP Server Configuration

KMIP (Key Management Interoperability Protocol) enables the secure creation and storage of keys and other security objects on a key management server.

> Note: You can also use an HSM (Hardware Security Module) to store the Admin Key. For details, see Hardware Security Modules with CSP Vault.

In addition, Cryptographic Security Platform Vault includes a fully functional KMIP server that you can use to serve requests from external KMIP clients. The Cryptographic Security Platform Vault KMIP server supports all KMIP versions up to 3.0. The KMIP server is required if you want to use Cryptographic Security Platform Vault with VMs and VSAN datastores encrypted by vSphere. For details, see CSP Vault with VSAN and VMware vSphere VM Encryption.

If you have linked Cryptographic Security Platform Vault with a Entrust CloudControl server version 5.1 or later, the Inventory feature in CloudControl provides an identifier that links each VM with its associated KMIP objects.

For details on KMIP, see the KMIP Technical Committee home page. For troubleshooting and error messages, see KMIP Errors and Troubleshooting.

- KEKs with KMIP
- Configuring a New KMIP Server
- Creating a Certificate Signing Request for KMIP Server
- Installing a Custom Certificate

KEKs with KMIP

A Key Encryption Key (KEK) provides an extra layer of security by encrypting all individual KMIP objects in a KMIP Vault. The KEK is created in your HSM for each KMIP vault and wraps all KMIP objects in the vault. Both the KEK and KMIP Vault must be available before a KMIP client can access the KMIP Vault.

To protect the KEK, the Cryptographic Security Platform Vault for KMIP requires that the KEK be stored in the hardware security module (HSM) associated with this Cryptographic Security Platform Vault for

KMIP cluster. If the HSM is not available, then the KMIP objects in the KMIP Vault protected by the KEK cannot be accessed. If you decide to associate a KEK with KMIP, it is imperative that the HSM be available to the Cryptographic Security Platform Vault for KMIP at all times.

The Cryptographic Security Platform Vault for KMIP uses the AES-GCM algorithm for encrypting and decrypting KMIP Vaults. Each KMIP object will be encrypted with a unique key derived from the KEK. The KEK can be cached in Cryptographic Security Platform Vault kernel memory by specifying the KEK cache timeout.

The KEK also provides a way to control the accessibility of all KMIP objects with a single command. If the KEK is revoked on the HSM, then all KMIP objects become inaccessible after the specified KEK cache timeout.

For information on configuring an HSM, see Hardware Security Modules with CSP Vault.

Considerations

- The HSM must be available before you can enable KEK for KMIP objects.
- After you enable KEK for KMIP objects, the HSM must be available anytime a KMIP object is accessed by a KMIP client.
- KMIP KEK can be enabled or disabled at any time.
    - When KMIP KEK is disabled, all KMIP objects will be decrypted. Key material will continue to be accessible.
    - If KMIP KEK is enabled and the HSM is disabled or unavailable, key material will not be accessible, but the UUID entries continue to be visible in WebGUI and object state can be changed.
- KMIP objects will remain accessible when encryption or decryption is in progress.

Configuring a New KMIP Server

Any KMIP client can connect to the Cryptographic Security Platform Vault KMIP server and perform all standard KMIP operations with the following restrictions:

- The Cryptographic Security Platform Vault for KMIP KMIP server supports KMIP versions 1.0, 1.1,1.2,1.3,1.4, 2.0, 2.1, and 3.0. The KMIP server protocol version is configured automatically and set between 1.0 to 3.0, as requested by the client.
- The object count (for example, keys) has a limit of 1 million KMIP objects per KeyControl Vault cluster. This limit includes all of the Cryptographic Security Platform Vault for KMIP instances in that cluster. If you exceed this limit, the KMIP server will still create and maintain the objects but the Cryptographic Security Platform Vault for KMIP webGUI may not display those objects correctly.

Important: Cryptographic Security Platform Vault includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When the first Cryptographic Security Platform Vault node is installed, it creates a Public CA that it also stores in the Cryptographic Security Platform Vault object store. For more information, see CSP Vault Certificates.
By default, the KMIP server uses a default certificate signed by the CA inside Cryptographic Security Platform Vault. This can be changed by installing a custom SSL certificate for the KMIP server. To generate a custom SSL certificate, you can use a CSR created from Cryptographic Security Platform Vault for the KMIP server (see Creating a Certificate Signing Request for KMIP Server) or you can use your own CSR. If you use your own CSR, you must upload a private key for that custom certificate.

For details about the standard KMIP operations and configuration settings, see the Oasis KMIP Technical Committee page or the KMIP wikipedia page.

When a KMIP client connects to the Cryptographic Security Platform Vault for KMIP KMIP server, the client must use the certificates associated with a KMIP server user account. The KMIP server does not support username/password login credentials. For details about downloading a user account certificate bundle, see Creating a KMIP Client Certificate.

Note:

- If you are configuring a KMIP server to use with VMware vSphere encryption or VSAN encryption, see the *Entrust KeyControl with VMware VSAN and vSphere VM Encryption* guide.
- If you are using a KMIP server with KEK enabled, please ensure that the KEK cache timeout is enabled. Set the value to anything other than 0.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI.
2. Select the Settings icon at the top right of the vault page.
3. On the KMIP Vault Settings page, complete the following:

Option	Description
State	If set to Enabled, clients can connect to this KMIP server.
Port	The server port number. The default port is 5696.
Verify	If set to Yes, the KMIP client identity is verified before the server handles its request. We recommend that you do not turn this option off.
Log Level	The lowest level of log messages that will be saved in the audit log. The options are: • **All**—Logs all requests to the KMIP server and responses from the KMIP server. • **Create-Modify**—Logs object creation, object modify requests, and object delete requests and responses. This is the default. • **Create-Get**—Logs object creation messages, object fetch requests, and object fetch responses. • **Create**—Logs object creation request and response messages. • **Get**—Logs object fetch and object locate requests and responses. • **Off**—No log messages are stored in the audit log.
TLS	Choose which version of TLS you want to support. If set to TLS 1.3, all clients must connect to this KMIP server using TLS 1.3. By default, both TLS 1.2 and TLS 1.3 are supported. Note: The TLS setting applies to the KMIP server only and affects the entire cluster.
Timeout	The length of time, in minutes, after which a client request will time out. If No is selected, client requests never time out. This is the default. To change this option, select Yesand select the number of minutes before the requests times out. This can be from 1 to 60 minutes.

Option	Description
KMIP Locate Operation: Maximum Items Default	Choose the maximum number of items to be returned from the KMIP server `Locate` operation. Note: The KMIP client allows you to set an offset items value (the record number the return starts with) and a maximum items value (how many items are returned) when you run the KMIP locate operation. The maximum number of items depends on both the choice that you set in the webGUI and the value that you set in the KMIP Client. For example: • If you choose the default value in the webGUI, and you DO set a max value in the KMIP Client, it returns up to 1000 UUIDs. • If you choose the default value in the webGUI, and you do NOT set a max value in the KMIP Client, it returns up to 100 UUIDs. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you DO set a max value, it returns the maximum value of UUIDs that is set in the KMIP Client. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you do NOT set max value, it returns all the UUIDs found in the locate operation. For more information on the KMIP `Locate` command, see https://docs.oasis-open.org/kmip/kmip-spec/.
SSL/TSL Ciphers	Enter the SSL ciphers in a comma-separated list that you want the KMIP server to use. Note: The following ciphers are not supported: DHE-DSS-AES128-256 and DHE-DSS-AES128-SHA256.

Option	Description
Certificate Types	This can be one of the following: If set to Default, the KMIP server uses a default certificate. If set to Custom, you must have a custom SSL certificate generated from Cryptographic Security Platform Vault or from your own CSR, and then provide the following: • SSL Certificate—Upload the SSL certificate file in Base64-encoded pem format. It should be able to function as a server certificate. • CA Certificate—Upload the certificate for the CA that signed the custom SSL certificate in Base64-encoded pem format. If you want to use the CA certificate to verify the KMIP client certificate select **Yes**. The default is **No**. **Important:** If you select Yes, you will need to upload a KMIP client certificate for every Cryptographic Security Platform Vault for KMIP. • Private Key—Optionally upload the private key file in Base64-encoded pem format. This is required if you used your own CSR and not the CSR generated on the KMIP page. • Password—Optionally enter the password for the custom certificate.

4. Click **Apply** and confirm your changes when prompted.

Creating a Certificate Signing Request for KMIP Server

A certificate signing request (CSR) tells an external Certificate Authority (CA) that you want an SSL certificate generated and signed by that CA. The SSL certificate can then be uploaded to Cryptographic Security Platform Vault and used in place of the default self-signed certificate.

When you use Cryptographic Security Platform Vault to create the CSR, Cryptographic Security Platform Vault creates a key pair and uses that key pair in conjunction with the information you specify to create the CSR. Cryptographic Security Platform Vault then encrypts the key pair and stores it for later use.

You can use the resulting CSR to generate an SSL certificate from the external CA you want to use. After you receive the SSL certificate from that external CA, you can upload it to Cryptographic Security Platform Vault. Because the key pair already exists on the system, you do not need to upload anything else.

If you create the CSR outside of Cryptographic Security Platform Vault, you need to upload both the SSL certificate and the matching private key file when you install the certificate on Cryptographic Security Platform Vault.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. Click the **Settings** icon.
3. On the KMIP Vault Settings page, select **Actions > Generate CSR**.
4. In the Generate Certificate Signing Request dialog box, specify the options you want to use.

Field	Description
Common Name	The name to associate with this request.
Locality	The locale to associate with this request.
State	The state to associate with this request.
Subject Alternative Names	The host names that will be protected by this certificate.
Key Size	Select the key size that you want to use. The default is 4096 bytes.
Country	The country to associate with this request. The default is US.
Organization	The organization to associate with this request.
Organization Unit	The organizational unit associate with this request.

5. Click **Generate**.
6. When you receive the message that Cryptographic Security Platform Vault has created the CSR, click **Download** to save a copy of the CSR to your browser's default download directory.
7. Use the CSR to request an SSL certificate from the external Certificate Authority you want to use. How you do this depends on the CA that you are using.

What to Do Next

After you receive the SSL certificate from the external CA, install it on Cryptographic Security Platform Vault. For more information, see Installing a Custom Certificate.

Installing a Custom Certificate

Before You Begin

Installing a custom certificate requires that you have at least your SSL certificate and CA certificate.

Note:

- When you use Cryptographic Security Platform Vault to create a CSR, and then use that CSR to generate an SSL certificate from the external CA you want to use, you will need to upload the CA certificate and the SSL certificate.
- If you create the CSR outside of Cryptographic Security Platform Vault, you will need to upload the CA certificate, the SSL certificate, and the matching private key file for the SSL certificate. If the private key file is encrypted, you will also need to enter the password used to decrypt the private key.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. Click **Settings**.
3. Under KMIP Vault Settings section, select **Enabled** to make changes.
4. In the Certificate Types field, select the **Custom** radio button.

5. In the SSL Certificate field, click **Browse**, select your SSL certificate, and then click **Open**.
6. In the CA Certificate field, click **Browse**, select your CA certificate, and then click **Open**.
7. Choose whether or not to use this CA certificate to verify your KMIP client certificate.
   Note: If you select **Yes**, then all existing KMIP client certificates in the individual KMIP vaults will no longer work. Vault Administrators will be required to upload a new KMIP client certificate, signed by this CA certificate, within their respective KMIP vaults. Until the Vault Administrators upload the new certificate, their vaults will not be able to communicate with the Cryptographic Security Platform Vault KMIP server.
   Important: If you change this value to **Yes**, the only way to set this back to **No** is to reset the KMIP server.
8. In the Private Key field, click **Browse**, select your private key, and then click **Open**.
   Note: This is only required if you created your SSL certificate outside of Cryptographic Security Platform Vault.
9. In the Password field, enter the password to decrypt your private key.
   Note: This is only required if you created your SSL certificate outside of Cryptographic Security Platform Vault, and the private key is encrypted.
10. Click **Apply** to overwrite the KMIP Server settings.

Hardware Security Modules with CSP Vault

A hardware security module (HSM) is a physical device that stores, protects, and manages cryptographic material. An HSM is often used to do cryptographic processing as well, including the generation of secure cryptographic keys. It is used in a client-server environment, which means that the server and the client each need to be prepared in advance. Using an HSM allows you to protect cryptographic keys and data, such as the Admin key and information you have stored in your vaults.

If you use multiple HSM servers and/or Cryptographic Security Platform Vault nodes to provide high availability of your services, you must ensure that all HSM servers are accessible from each Cryptographic Security Platform Vault instance.

When you configure an HSM, it does not automatically immediately start to protect data. You must regenerate the Admin key if you wish to store it in the HSM, and a Vault Admin must enable HSM protection in any vault where you want the HSM to protect keys or other material. See the documentation for the particular vault type:

- Cryptographic Security Platform Vault for Cloud Keys—Managing Key Sets.
- Cryptographic Security Platform Vault for KMIP—KEK with a KMIP Vault.
- Cryptographic Security Platform Vault for Secrets—Hardware Security Modules with CSP Vault for Secrets.
- Cryptographic Security Platform Vault for Databases—Configuring a CSP Vault Database Connector, Configuring CSP Vault for Oracle TDE, Configuring CSP Vault for MariaDB TDE, Creating a Cloud VM Set for the CSP Vault for Databases
- Cryptographic Security Platform Vault for Cryptographic APIs—Signing in to the Vault for the First Time.
- Cryptographic Security Platform Vault for VM Encryption—KEKs with Cloud VM Sets, Creating a Cloud VM Set for the CSP Vault for VM Encryption.

If using an Entrust nShield HSM you can also configure it as a root of trust for the system. For more information, see Adding HSM Root-of-Trust to nShield Server .

When an HSM is used with BYOK, keys are never stored as plaintext. In-memory keys are also encrypted (wrapped), except for software-protected keys in Azure. When a software-protected key has to be uploaded to Azure, Cryptographic Security Platform Vault unwraps it before upload. For other keys, including hardware-protected keys on Azure, when Cryptographic Security Platform Vault has to upload them to the cloud, it encrypts (wraps) them in the HSM using the master key and the cloud provider's wrapping key before uploading the wrapped keys to the cloud.

Cryptographic Security Platform Vault supports the following HSMs:

- nShield HSM

- nShield as a Service (nSaaS)
- Luna HSM
- Luna Cloud HSM

Requirements and Recommendations for nShield HSM Servers

The nShield HSM client version 13.9.0 is included in Cryptographic Security Platform Vault. Only nShield HSMs compatible with the 13.9.0 client are supported. The minimum HSM firmware version for BYOK, KEK generation, and TDE is 12.70. You can also use either the on-premise nShield HSM or nShield as a Service (nSaaS).

> Note: Elliptic Curve Cryptography (ECC) was an optional feature on nShield HSMs with firmware versions before 13.5. In order to use such HSMs with the Cryptographic Security Platform Vault for Cloud Keys or the Cryptographic Security Platform Vault for Cryptographic APIs containing Elliptic Curve Keys, you must have the feature enabled. You can check the feature status using the HSM's `fet` command.

The following details apply where nShield HSMs are configured in a FIPS 140-2 Level 3 compliant Security World environment:

Security World Files—For each nShield HSM, the following files must be present and up to date in Cryptographic Security Platform Vault. These files are supplied in the world.zip file uploaded when configuring the HSM:

- `world`
- A `module_<ESN>` file for each module that Cryptographic Security Platform Vault uses
- A `cards_<IDENT>` file for each card set that is to be used
- A `card_<IDENT>_<NUMBER>` file for each card in each card set that is to be used to provide FIPS authorization

These files are not updated automatically. You must ensure that they are synchronized whenever the Security World is updated on the module. For more information, see 'Creating a Security World' in your HSM User Guide. The updated files should be in included in a world.zip archive and updated using the 'Upload Security World' action on the nShield HSM Server Settings page.

Important: The Security World must be created for nShield client software version 13.6.3 or later.

Smart cards—When using an nShield HSM with a FIPS 140-2 Level 3 Security World, a FIPS authorization token is required to authorize most operations, including the creation of keys. This is provided by an ACS or OCS card must be loaded in the HSM or presented using a remote admin client. Cards are usually configured when setting up an HSM, so Entrust recommends leaving one of the configured OCS cards in the HSM slot to satisfy this requirement.

Smart card serial numbers—nShield HSMs include a security feature that checks the serial numbers of the cards as well as checking they are part of an OCS for this HSM. This allows the admin to disable a card that is mislaid for example. In Cryptographic Security Platform Vault, you can specify whether all cards are accepted, no cards are accepted, or cards in a specific list are accepted. Card serial numbers are 16 decimal digits and, if you enable the option, Cryptographic Security Platform Vault checks that the card in use matches one of the serial numbers listed.

For additional details, see your nShield documentation https://nshielddocs.entrust.com/ or the nShield support site https://nshieldsupport.entrust.com.

Requirements and Recommendations for Luna HSM Servers

You can configure the nodes in your Cryptographic Security Platform Vault cluster to either connect to the HSM using one certificate that they all share or with individual certificates for each node. The Cryptographic Security Platform Vault nodes can also be connected to multiple HSM servers that have been configured as

an HA Group to allow for High Availability. For more information, see Configuring Cryptographic Security Platform Vault as a Luna HSM Client with a Single Cluster Certificate, Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates, and Configuring a Luna HSM HA Group.

> Note: If you have a Luna HSM server with the `ipcheck` feature enabled, you must use unique node certificates.

- The Luna client version 10.9.0 is included in Cryptographic Security Platform Vault. This version of the Luna HSM client is compatible with Luna HSMs with firmware 6.2.1 or higher.
- Bandwidth recommendation:
  - Minimum: 10 Mbps half duplex
  - Recommended: 100 Mbps full duplex
- Latency recommendation:
  - Maximum: 500 ms
  - Recommended: 0.5 ms
- TCP port 1792 is required to establish a trusted connection between Cryptographic Security Platform Vault and Luna. The other ports used are:
  - TCP port 22 for SSH (Secure Shell).
  - TCP port 1503 for Remote PED. This is the only configurable port.
  - UDP port 514 for the Syslog service.
  - UDP port 123 for NTP service.
  - UDP ports 161/162 for SNMP service.

For additional details, see your Luna HSM documentation.

- Adding a CSP Vault Node to a Cluster using an nShield HSM client
- Configuring CSP Vault as an HSM Client using an nShield HSM
- Adding HSM Root-of-Trust to nShield Server
- Running nShield HSM Info Commands in the webGUI
- Configuring an nShield HSM for High Availability
- Replacing an nShield HSM on a CSP Vault Cluster
- Configuring Allowed Smart Cards for an nShield HSM
- KeySafe5 Agent Requirements
- Enabling the KeySafe5 Agent
- Configuring CSP Vault as a Luna Cloud HSM Client
- Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate
- Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates
- Configuring a Luna HSM HA Group
- Adding a CSP Vault Node to an Existing Luna HSM Configuration
- Adding a New Luna HSM to an Existing Luna HSM Configuration
- Adding a Luna Cloud HSM to an Existing Luna HSM Configuration
- Changing the Luna Client Certificate Mode
- Locating the HSM Server Admin Key
- Resetting the HSM Server Configuration

Adding a CSP Vault Node to a Cluster using an nShield HSM client

After you have configured a single node cluster for the nShield HSM, you can quickly add a new Cryptographic Security Platform Vault node. All members of the Cryptographic Security Platform Vault cluster must be added as clients of the nShield HSM server(s).

1. Use the webGUI to join the new node to your existing cluster that is configured with nShield HSM. For complete instructions, see Joining or Re-joining a Cryptographic Security Platform Vault Cluster.
2. After the process is finished, log in to the new cluster node using the webGUI.
3. In the **System Settings** section, click **HSM Server Settings**.

4. On the **HSM Server Settings** tab, select **nShield HSM**.
   You should see the nShield HSM Server Settings page with all of the settings imported from the original cluster node.
5. Click the **Client List** tab to view the cluster nodes.
6. Copy the Cryptographic Security Platform Vault IP address and the keyhash of the node that you just added, and paste them in a text window.
7. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node, and authenticate each node to each HSM.
8. Return to the nShield HSM Server Settings page for the new cluster node.
9. Click the **Locate Admin Key** button to ensure that the new node is now fully connected to nShield HSM.

Configuring CSP Vault as an HSM Client using an nShield HSM

The following procedure describes how to configure Cryptographic Security Platform Vault as an nShield HSM client. You can either use a standalone Cryptographic Security Platform Vault node or a cluster.

Before You Begin

For the nShield HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM Server Name, Server IP/FQDN, ESN, Port, and Keyhash.
- The Security World Bundle file that is provided by the HSM Administrator. This must contain the following:
  - The world file.
  - The module file for each HSM server you plan to use.
  - If it is a FIPS Level 3 security world, the card files for any smartcards that will be used to provide FIPS authorization.
- Information to create a softcard consisting of a label and password.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- If you are using an on-premise HSM server, you must have access.

If you plan to use a FIPS 140-2 Level 3 compliant Security World environment, see Hardware Security Modules with CSP Vault for more information.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
   Note: If you are using a cluster, you only need to use the Cryptographic Security Platform Vault Management webGUI for one node.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **HSM Server Settings** tab, select **Entrust nShield HSM**.
   The nShield HSM Server Settings window displays the information you will need to continue.
6. Click the **Copy the IP address and keyhashes to the keyboard** link and paste them in a text window.
7. Copy the Security World Bundle from nShield and place it on your local machine. It should be in the format world.zip.
8. After reading the Get Started Screen, click **Continue**.
9. On the Enrollment screen, complete the following:

Note: All information is from the nShield HSM. The Server Name is used for display purposes and the Server IP/FQDN is used for communication.

Field	Description
Server Name	Enter the FQDN of the nShield HSM.
Server IP	Enter the IP address for the nShield HSM.
Server ESN	Enter the nShield Electronic Serial Number (ESN).
Port	Enter the port used for the nShield HSM.
Keyhash	Enter the keyhash of the nShield HSM.

10. Click **Enroll and Continue**.
11. On the Security World screen, click **Browse** and locate the security world bundle that you downloaded from the nShield HSM.
12. Click **Upload and Continue**.
13. If you are using a FIPS 140-2 Level 3 Security World, on the Card List screen, select one of the following:
    - Accept all cards—Accepts all nShield Remote Administration smart cards.
    - Add Specific cards—Accepts specific nShield Remote Administration smart cards. To add a card, click **+ Add Card**, enter the card serial number and optional description, check the Enable checkbox, and click **Add**. You can add multiple cards at one time.
14. If you are using a FIPS 140-2 Level 3 Security World, on the Softcard screen, enter the Softcard Label and Softcard Password that you want to use to link to the HSM server.
    You must have entered a valid smart card or selected Accept all cards in order to create a Softcard. The Softcard Label and Softcard Password must meet the following requirements:
    Softcard Label
    - At least 8 characters
    - No more than 31 characters
    - Can include uppercase, lowercase, numbers, and special characters
    - No space or tab character

    Softcard Password
    - At least 8 characters
    - No more than 127 characters
    - At least 1 uppercase
    - At least 1 lowercase
    - At least 1 number
    - No space or tab character
15. Click **Complete Setup**.
    After the setup is complete, you will be returned to the nShield HSM Server Settings page.
    Note: If the configuration failed, then you must select **Actions > Reset HSM Configuration** before you try again.
16. Select **Actions > Test Connection** from the Basic tab to ensure that the HSM is fully connected to Cryptographic Security Platform Vault.

What to Do Next

- If you want to use nShield HSM to store your Admin Key, you will need to generate a new one.
  See Generating the Admin Key.

The new Admin Key is automatically stored in the nShield HSM. Click **Locate Admin Key** in the nShield HSM Server Settings page to view.

- If you want to use HSM Root-of-Trust, see Adding HSM Root-of-Trust to nShield Server .
- If you want to form a Cryptographic Security Platform Vault cluster using the nShield HSM, see Adding a CSP Vault Node to a Cluster using an nShield HSM client.
- If you want to use an additional nShield HSM for a high availability cluster, see Configuring an nShield HSM for High Availability.
- If you want to use KeySafe5, see Enabling the KeySafe5 Agent.

Adding HSM Root-of-Trust to nShield Server

HSM Root-of-Trust provides enhanced protection for the contents of the object store. Root-of-Trust is gained when the HSM provides the cryptographic keys necessary to unlock the object store.

If the HSM cannot be contacted when Cryptographic Security Platform Vault boots, or if the correct keys cannot be located, trust cannot be established with the HSM and Cryptographic Security Platform Vault is not allowed to begin servicing key requests.

Important: Creating an HSM Root-of-Trust is not reversible. Once the HSM Root-of-Trust is enabled, you cannot remove the HSM. Contact Entrust Support to disable it.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, select the HSM Root-of-Trust mode that you want to use:
    - Root-of-Trust mode using HWSIG—The hardware signature is used to wrap the HSM configuration file. Unless there is a change to Cryptographic Security Platform Vault's hardware configuration, booting Cryptographic Security Platform Vault will require no user intervention before it can begin servicing requests.
      Virtual machine configuration changes may result in a need to recover the HSM configuration changes. When this happens, the normal Cryptographic Security Platform Vault Masterkey Recovery procedure is used. This requires the softcard label and password if the admin key is stored in the HSM, or the downloaded admin key if it is not stored in the HSM.
    - Root-of-Trust mode using Password—The HSM's softcard password is used to wrap the HSM configuration file. When Cryptographic Security Platform Vault boots, the WebGUI will prompt for the HSM password. Only when the password is correctly entered is Cryptographic Security Platform Vault allowed to begin booting.
      The HSM password must be entered on each node of the cluster. For instance, if the entire cluster is restarted, read-only operations will start on each node as soon as it has finished booting, but the cluster will be degraded until the password has been entered on all of the nodes in the cluster, and the nodes are back up.
6. Select the HSM Root-of-Trust Timeout value in minutes and click **Save**. The default timeout value is 0, which means the nodes will never be locked down, but will be checked at boot time.
   You can select up to 1440 minutes (1 day).
   Note: If the node is unable to connect to any HSM server, and still cannot connect after the timeout period, that Cryptographic Security Platform Vault node will be locked down and will not respond to any requests via the webGUI or API. Diagnostic logs are available from the system console using the Cryptographic Security Platform Vault System Console. After resolving the connection issue, reboot the Cryptographic Security Platform Vault node to re-enable it.
   When using the System Console to download the diagnostic logs, you will see the message “Cryptographic Security Platform Vault not initialised yet. Proceeding may potentially leave the system unusable.” This is expected, and enabling the htrestricted account will not cause a problem.

7. Click **Apply**.

Running nShield HSM Info Commands in the webGUI

You can run several Info commands against your nShield HSM directly from the webGUI.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Select **Actions > Run Info Commands**.
6. In the Run Info Commands window, select the command that you want to run and click **Apply**.
   The standard output and error output (if applicable) are displayed.

Configuring an nShield HSM for High Availability

After you have configured Cryptographic Security Platform Vault as an nShield HSM client, you can add an additional nShield HSM to create a high availability cluster. You can either use a standalone Cryptographic Security Platform Vault node or a Cryptographic Security Platform Vault cluster.

When the Cryptographic Security Platform Vault cluster is configured with multiple HSM servers, the Cryptographic Security Platform Vault cluster uses HSM servers for High Availability (HA) and load sharing purposes. The HSM servers are not affiliated with specific Cryptographic Security Platform Vault node(s), but are configured for and used by ALL members of the Cryptographic Security Platform Vault cluster.

Before You Begin

- Ensure that you have completed Configuring CSP Vault as an HSM Client using an nShield HSM.
- Obtain the Security World Bundle file for the new HSM that you want to add. It must have the same security world as the first HSM server inside of the Security World Bundle file, but the module file must be for the new HSM. Please contact your HSM Administrator to ensure that this is set up correctly.
  You cannot establish HA functionality if the servers do not share the same security world.
  Tip: For more information, see the 'Security Worlds' and 'Creating and Managing a Security World' chapters of your nShield Connect User Guide.

FIPS 140-2 Level 3 – smart card requirement

If your nShield HSMs are configured in a FIPS 140-2 Level 3 compliant Security World environment, an ACS or OCS card must be loaded in all HSMs. When using multiple HSMs for high availability, operations are load balanced between the HSM servers connected to Cryptographic Security Platform Vault. If one HSM fails, traffic is rerouted to another HSM. If a valid card is not located in the HSM, it will continue to receive traffic but operations requiring a FIPS authorization token will fail. A valid card (with a listed serial number, unless 'Accept all cards' is selected) must be loaded in the HSM to ensure operations do not fail. For more information regarding nShield HSMs and FIPS 140-2 Level 3, see Hardware Security Modules with CSP Vault

> Note: If you wish to use OCS cards that were not included in the security world bundle previously uploaded, ensure that the corresponding card files are included in the new bundle.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.

5. On the nShield HSM Server Settings page, click the **Client List** and copy the IP address and keyhash of the Cryptographic Security Platform Vaultnodes.
6. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node.
7. Copy the Security World Bundle from nShield and place it on your local machine. It should be in the format world.zip.
8. On the Server List tab of the nShield HSM Server Settings page, select **Actions > Add New HSM Server**.
9. After reading the Get Started Screen, click **Continue**.
10. On the Enrollment screen, complete the following:
    Note: All information is from the nShield HSM. The Server Name is used for display purposes and the Server IP/FQDN is used for communication.

Field	Description
Server Name	Enter the FQDN of the nShield HSM.
Server IP/FQDN	Enter the IP address or FQDN for the nShield HSM.
Server ESN	Enter the nShield Electronic Serial Number (ESN).
Server Port	Enter the port used for the nShield HSM.
Server Keyhash	Enter the keyhash of the nShield HSM.

11. Click **Enroll and Continue**.
12. On the Security World screen, click **Browse** and locate the security world bundle that you downloaded from the nShield HSM.
13. Click **Upload and Continue**.
14. If you are using a FIPS 140-2 Level 3 Security World, on the Card List screen, select one of the following:
    - Accept all cards—Accepts all nShield Remote Administration smart cards.
    - Add Specific cards—Accepts specific nShield Remote Administration smart cards. To add a card, click **+ Add Card**, enter the card serial number and optional description, check the Enable checkbox, and click **Add**. You can add multiple cards at one time.
15. Click **Complete Setup**.
    After the setup is complete, you will be returned to the nShield HSM Server Settings page, which now displays the values for both HSMs on the Server List tab.
    Note: If the configuration failed, then you can simply remove the HSM by selecting it and then selecting **Actions > Remove Server** and add it again.

Replacing an nShield HSM on a CSP Vault Cluster

If you have a Cryptographic Security Platform Vault cluster on an nShield HSM, you can replace the HSM while maintaining the cluster. This procedure documents a 2-node cluster. If you have more than two nodes you will need to modify the instructions.

Before You Begin

To replace the nShield HSM, make sure you have the following information available:

- The HSM server name, server IP/FQDN, ESN, Port, and Keyhash for the replacement nShield HSM (HSM-2).

- The Security World Bundle file for the replacement HSM. Both HSM-1 and HSM-2 must have the same security world inside of the Security World Bundle file. Please contact your HSM Administrator to ensure that this is set up correctly.
  Tip: This information can be found in the sections on replacing, adding, or restoring an HSM to the Security World in chapters 2 and 9 of the nShield® Connect User Guide for Unix.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, click the **Client List** tab.
6. Copy the Cryptographic Security Platform Vault IP addresses and keyhashes to notepad. You will need the IP address and keyhash of both the Cryptographic Security Platform Vault nodes (node-1 and node-2) to authenticate Cryptographic Security Platform Vault on the replacement nShield HSM (HSM-2).
7. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node.
8. Copy the Security World Bundle from the replacement HSM-2 as world.zip and place it on your local machine.
9. On the nShield HSM Server Settings, click the **Server Settings** tab and then select HSM-1.
10. Replace the Server Name, Server IP/FQDN, Server ESN, Server Port and Server Keyhash of HSM-1 with the values for HSM-2.
11. Click **Apply**.
12. Select **Actions > Upload Security World** and upload the security world bundle for HSM-2.
13. Test your connection with HSM-2.

Configuring Allowed Smart Cards for an nShield HSM

When using an nShield HSM with a FIPS 140-2 Level 3 Security World a FIPS authorization token is required to authorize most operations, including the creation of keys. This is provided by an ACS or OCS card which must be loaded in the HSM or presented using a remote admin client. Cards are usually configured when setting up an HSM, so Entrust recommends leaving one of the configured OCS cards in the HSM slot to satisfy this requirement.

nShield HSMs include a security feature that checks the serial numbers of the cards as well as checking they are part of an OCS for this HSM. This allows the admin to disable a card if necessary.

The Card List tab of the nShield HSM Server Settings page In the Cryptographic Security Platform Vault Management webGUI allows you to control which card serial numbers are accepted. The tab is only available if the HSM is using a FIPS 140-2 Level 3 Security World and displays the current setting and details of any card serial numbers you have entered.

There are 3 basic modes:

- Accept All Cards—Does not check the card serial number. You can enter or leave this mode by selecting **Actions > Accept All Cards**. If the entry in the menu is preceded by a checkmark, it is enabled. Select **Actions > Accept All Cards** to disable.
- Reject All Cards—Does not allow any cards, so all operations requiring one will fail. You can enter or leave this mode by selecting **Actions > Reject All Cards**. If the entry in the menu is preceded by a checkmark, it is enabled. Select **Actions > Reject All Cards** to disable.

- Allow listed enabled cards—If neither of the modes is selected, any cards in the list that are Enabled will be allowed, and all other cards will be rejected.

Select a card from the list and then select a choice from the actions menu to delete, disable, or enable the selected card. You can add a card to the list by selecting Actions > Add Card. You can also add or edit a description for a card.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **nShield HSM Server Settings** page, select the Card List tab.
6. Add or update your cards as necessary.

KeySafe5 Agent Requirements

Beginning with 10.5.3, you can use KeySafe5 for your nShield HSMs using the Cryptographic Security Platform Vault Management webGUI and Cryptographic Security Platform Compliance Manager webGUI. KeySafe5 contains an agent that runs on HSM clients and a GUI that allows remote management of setup and configuration tasks, provides visibility into the status of your nShield Security World, and allows real-time and historical monitoring.

To use KeySafe5 GUI, you must have the following:

- An nShield HSM must be enabled.
- Your Cryptographic Security Platform Vault Management webGUI must be connected as an Appliance Cluster in the Cryptographic Security Platform Compliance Manager webGUI.
- Anytime your Cryptographic Security Platform Compliance Manager is disconnected and reconnected, you will need to disable and re-enable the KeySafe5 agent in the Cryptographic Security Platform Vault Management webGUI.
- The KeySafe5 agent only runs on the primary node of the cluster.
- When you view the KeySafe5 GUI, the agent appears with the hostname of the cluster primary node. Even if you delete the primary node, the KeySafe5 agent name remains the same in the KeySafe5 GUI.
- After you enable the agent in the Cryptographic Security Platform Vault Management webGUI, it may take up to 15 minutes for the data to sync to the KeySafe5 GUI.
- After enabling the agent in the Cryptographic Security Platform Vault Management webGUI, you will need to log in to the Cryptographic Security Platform Compliance Manager webGUI, navigate to Data Sources, launch the KeySafe5 GUI, and perform the "reveal metadata" operation before your HSM keys will appear in the Cryptographic Security Platform Compliance Manager.

Enabling the KeySafe5 Agent

You need to enable the KeySafe5 agent in the Cryptographic Security Platform Vault Appliance before you can use it.

Before You Begin

- Ensure that an nShield HSM is properly configured in your Cryptographic Security Platform Vault Appliance. For more information, see Configuring CSP Vault as an HSM Client using an nShield HSM.
- Ensure that your Cryptographic Security Platform Vault Appliance webGUI is connected to the Cryptographic Security Platform Compliance Manager as an Appliance Cluster. For more information, see Connecting CSP Vault and CSP Compliance Manager.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, set the KeySafe5 Agent to **Enable**.
6. Click **Apply**.
7. Navigate to the Compliance Manager page where you connected to the Cryptographic Security Platform Compliance Manager webGUI and click **Sync Now**.

Configuring CSP Vault as a Luna Cloud HSM Client

The following procedure describes how to configure Cryptographic Security Platform Vault as a Luna Cloud HSM Client.

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The service client bundle for the HSM. When you create a service client, you will be prompted to download the service client bundle.
- The HSM partition name and password.
- A Cryptographic Security Platform Vault account with Security Admin privileges.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
6. On the **Luna HSM Server Settings** page, select the **Luna Cloud HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.
Crypto Officer (CO) Password	Enter the password for the Crypto Officer (CO) password.

Field	Description
Service Client Bundle	Click Browse to specify the location of the service client bundle that you downloaded.
Session Timeout	The length of time Cryptographic Security Platform Vault keeps the communication session open with an HSM server. When the session expires, a new session is created with the same timeout value. The default is 30 minutes.

7. Click **Apply**, then click **Proceed** at the prompt.
8. Select **Actions > Test Connection** to test your connection. You should see a message that says the HSM connection is OK.

Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate

When you connect a Cryptographic Security Platform Vault cluster to a hardware security module (HSM), you can create one certificate for the Cryptographic Security Platform Vault cluster that you can use for all Cryptographic Security Platform Vault nodes or you can have an individual certificate for each node in the Cryptographic Security Platform Vault cluster.

Important: If you have a Luna HSM server with the `ipcheck` feature enabled, you must use Individual Node Certificates for Client Certificate Mode.

The following procedure describes how to configure Cryptographic Security Platform Vault as an HSM client that uses a single certificate for the entire cluster. If you want to use individual certificates for each node, see Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates.

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password.
- The client name you want to assign to the Cryptographic Security Platform Vault cluster.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

Note: The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the HSM server to which you want to connect. We recommend that you rename the `server.pem` certificate file so that you can find the certificate file easily when you need to upload it to Cryptographic Security Platform Vault later in this procedure.
   For example, if your HSM server is `hsm1.my-company.com`, you could enter:

```
# scp admin@hsm1.my-company.com:server.pem ./hsm1cert.pem
admin@hsm1.my-company.com's password:

server.pem          100% 1155     1.1KB/s   00:00
```

2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.
6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the **Luna HSM Server Settings** page, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Hostname	Enter the hostname for the HSM server.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.
Partition or Crypto Officer (CO) Password	Enter the password for the Cryptographic Security Platform Vault partition or the Crypto Officer (CO) password for Luna HSM modules version 7 and above.
Server Certificate	Click Browse to specify the location of the HSM server certificate file.
Session Timeout	The length of time Cryptographic Security Platform Vault keeps the communication session open with an HSM server. When the session expires, a new session is created with the same timeout value. The default is 30 minutes.
Client Certificate Mode	Select the Single Cluster Certificate radio button so that Cryptographic Security Platform Vault will use the same certificate for all nodes in the cluster.
Client Name	Specify a name for the Cryptographic Security Platform Vault client on the HSM server. This name must be unique on the HSM server.
Admin Key ID	Indicates whether an Admin Key already exists on the HSM.

8. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.

9. Select **Actions > Generate Client Certificate** to download the cluster certificate that all Cryptographic Security Platform Vault nodes can use. Cryptographic Security Platform Vault automatically saves *client-name*.pem file to your browser's default download location.
   For example, if you use the default client name KC_Cluster, the cluster certificate name would be KC_Cluster.pem.
10. Upload the cluster certificate to the root directory on the HSM server. For example:
    ```
    # scp KC_Cluster.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC_Cluster.pem          100% 1164     1.1KB/s   00:00
    ```
11. Using a shell account, log into the HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using the same client name you specified in the webGUI for both the client name and hostname.
       Tip: If the registration fails because a client of that name already exists, you either need to delete the existing client or go back to the webGUI, enter an new client name, click **Apply**, and then download a new cluster certificate that you can upload to the HSM server.
    b. Assign any partitions that you intend to use to the Cryptographic Security Platform Vault client.
       Note: This should include the partition specified above and any others that you intend to use from CSP Vaults.

    For example, if you want the Cryptographic Security Platform Vault client KC_Cluster to be assigned to KC_partition1 on hsm1.my-company.com, you could enter:
    ```
    # ssh admin@hsm1.my-company.com
    admin@hsm1.my-company.com's password:

    [hsm1] lunash:>client register -client KC_Cluster -hostname KC_Cluster
    'client register' successful
    Command Result : 0 (Success)
    [hsm1] lunash:>client assignPartition -client KC_Cluster -partition KC_partition1
    'client assignPartition' successful
    Command Result : 0 (Success)
    [hsm1] lunash:>exit
    ```
12. Return to the **Luna HSM Server Settings** page and click **Test**. You should see a message that says the HSM connection is OK and that the Admin Key needs to be regenerated.
    To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.

Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

When you connect a Cryptographic Security Platform Vault cluster to a hardware security module (HSM), you can create one certificate for the Cryptographic Security Platform Vault cluster that you can use for all Cryptographic Security Platform Vault nodes or you can have an individual certificate for each node in the Cryptographic Security Platform Vault cluster. If you have a Luna HSM server with the ipcheck feature enabled, you must use unique node certificates.

The following procedure describes how to configure Cryptographic Security Platform Vault as an HSM client that uses unique certificates for each node in the cluster. If you want to use a single certificate that will be shared by all nodes in the cluster, see Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the HSM server to which you want to connect. We recommend that you rename the `server.pem` certificate file so that you can find the certificate file easily when you need to upload it to Cryptographic Security Platform Vault later in this procedure.
   For example, if your HSM server is `hsm1.my-company.com`, you could enter:
   ```
   # scp admin@hsm1.my-company.com:server.pem ./hsm1cert.pem
   admin@hsm1.my-company.com's password:

   server.pem          100% 1155     1.1KB/s   00:00
   ```
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.
6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the**Luna HSM Server Settings** page, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Hostname	Enter the hostname for the HSM server.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.

Field	Description
Partition or Crypto Officer (CO) Password	Enter the password for the Cryptographic Security Platform Vault partition or the Crypto Officer (CO) password for Luna HSM modules version 7 and above.
Server Certificate	Click Browse and open the appropriate HSM server certificate file.
Client Certificate Mode	Select the Individual Node Certificates radio button so that Cryptographic Security Platform Vault will use a unique certificate for each node in the cluster.
Admin Key ID	Indicates whether an Admin Key already exists on the HSM.

8. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.
9. Navigate to the **Client List** tab. You should see one entry for each Cryptographic Security Platform Vault node in the cluster.
10. Select the first node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called `node-name.domain-name.pem` and downloads it to your browser's default download location.
    For example, if the name of the node is `KC-1` and it is running on the domain `my-company.com`, the certificate file would be called `KC-1.my-company.com.pem`.
11. Repeat the previous step for each Cryptographic Security Platform Vault node in the cluster.
12. Upload all certificates to the root directory on the HSM server. For example, if you have two Cryptographic Security Platform Vault nodes, you would copy both Cryptographic Security Platform Vault node certificates to HSM server:
    ```
    # scp KC-1.my-company.com.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC-1.my-company.com.pem          100% 1164     1.1KB/s   00:00

    # scp KC-2.my-company.com.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC-2.my-company.com.pem          100% 1164     1.1KB/s   00:00
    ```
13. Using a shell account, log into the HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using `"node-name.domain-name"` for both the client name and hostname. The double quotes are required because of the period in the client name.
       Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the name of the client pem file that CSP Vault generates.
    b. Assign any partitions that you intent to use to the Cryptographic Security Platform Vault client.
       Note: This should include the partition that you specified above as well as any other partitions that you intent to use from CSP Vaults.

    For example, if you want the Cryptographic Security Platform Vault client to be assigned to `KC_partition1` on `hsm1.my-company.com`, you could enter:

```
# ssh admin@hsm1.my-company.com
admin@hsm1.my-company.com's password:

[hsm1] lunash:>client register -client "KC-1.my-company.com" -hostname "KC-1.my-company.com"

'client register' successful
Command Result : 0 (Success)
[hsm1] lunash:>client register -client "KC-2.my-company.com" -hostname "KC-2.my-company.com"

'client register' successful
Command Result : 0 (Success)
[hsm1] lunash:>client assignPartition -client "KC-1.my-company.com" -partition KC_partition1
'client assignPartition' successful
Command Result : 0 (Success)
[hsm1] lunash:>client assignPartition -client "KC-2.my-company.com" -partition KC_partition1
'client assignPartition' successful
Command Result : 0 (Success)
[hsm1] lunash:>exit
```

14. Return to the **LunaHSM Server Settings** page and click **Test**. You should see a message that says the HSM connection is OK and that the Admin Key needs to be regenerated.
    To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.

Configuring a Luna HSM HA Group

If you want to connect a Cryptographic Security Platform Vault cluster to multiple HSM servers, you must create an HA group for those servers on *each*Cryptographic Security Platform Vault node in the cluster. That way any Admin Keys or KEKs that Cryptographic Security Platform Vault creates will be stored on all HSM servers in the group and can be accessed from any of the HSM servers by any of the Cryptographic Security Platform Vault nodes.

You can create a group with two or more Luna HSMs, or a single Luna Cloud HSM and one or more Luna HSMs.

Before You Begin

- Make sure you have configured the HSM servers in the Cryptographic Security Platform Vault webGUI and registered the Cryptographic Security Platform Vault clients with the HSM servers as described in Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate, Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates, or Adding a New Luna HSM to an Existing Luna HSM Configuration.
- Make sure the Luna HSM servers meet the Luna HSM requirements for membership in an HA group. The partitions you select for the HA Group must have the same CO password and be configured in Cloning Mode. For details about these requirements, see your Luna HSM documentation.

Procedure

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).

2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage HSM Client Account**.
3. From the Manage HSM Client Account page, select **Enable and Set Password for HSM Client Account**.
4. Acknowledge the password requirements at the prompt.
5. On the Change hsmadmin Password page, specify the password you want to use and select **OK**.
6. Select **Return to Main Menu**.
7. From the main Entrust Cryptographic Security Platform Vault System Console, select **Log Out**.
8. Log into the server as `hsmadmin` with the password you just specified. Wait until the Cryptographic Security Platform Vault node has retrieved the information about the registered HSM servers and has displayed the `lunacm:>` prompt. Depending on your network, it may take some time to retrieve this information.
9. Make sure that all HSM servers on which you registered the Cryptographic Security Platform Vault node, and the Luna Cloud HSM if you are using one, are displayed in the list with assigned Slot IDs and the correct partition labels.
   Important: If you do not see all of the HSM servers that you expect to see, do not continue with this step. Instead, use `exit` to return to the login prompt and then make sure that you have registered the Cryptographic Security Platform Vault node with all of the HSM servers you want to use.
10. Create an HA group according to your Luna HSM documentation. The following steps are shown for your convenience and may need to be changed based on the version of your Luna HSM server. The password you specify must be the password for the Luna HSM partitions you entered in the Cryptographic Security Platform Vault webGUI.

    ```
    lunacm:>haGroup createGroup -slot 0 -label hagroup -password HSMPartPswd
    Warning: There are objects currently on the new member.
    Do you wish to propagate these objects within the HA
    group, or remove them?

    Type 'copy' to keep and propagate the existing
    objects, 'remove' to remove them before continuing,
    or 'quit' to stop adding this new group member.
    >copy
    ```

    At this point, you should see messages stating that the HA group was created without error. If this succeeds, you can add all other HSMs to the HA group.

    ```
    lunacm:>haGroup addMember -slot 1 -group hagroup -password HSMPartPswd
    Warning: There are objects currently on the new member.
    Do you wish to propagate these objects within the HA
    group, or remove them?

    Type 'copy' to keep and propagate the existing
    objects, 'remove' to remove them before continuing,
    or 'quit' to stop adding this new group member.
    >copy

    Disable hagroup logging with
    lunacm:> hagroup halog -disable
    ```

    Repeat the `haGroup addMember` command for each additional HSM server until all HSM servers with which you registered this Cryptographic Security Platform Vault node are members of the HA group.
11. After all members have been added, use the `exit` command to log out of `hsmadmin`.
12. Repeat this procedure on all Cryptographic Security Platform Vault nodes in the cluster.
13. After you have created the HA group on *all* nodes in the cluster, go back to the Cryptographic Security Platform Vault webGUI HSM Server Settings page and do the following:
    a. Change the **Partition Label or HA Group Name** to be the name of the HA group you created.

Note: If your HA group contains both the Luna HSM and Luna Cloud HSM, you will need to update this field on both tabs on the Thales HSM Server Settings page. Do not generate a new admin key until both tabs have been updated and you have applied the changes.

b. Click **Apply**, then click **Proceed** at the prompt. You should see a message that the HSM hostname or partition label has changed and that you need to regenerate the Admin key. If this message appears then the connection to all of the HSM servers in the HA group succeeded.

c. To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > Luna HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.
Important: If your HA group contains both the Luna HSM and Luna Cloud HSM, do not generate a new admin key until both tabs have been updated and you have applied all of the changes.

Adding a CSP Vault Node to an Existing Luna HSM Configuration

How you add a new Cryptographic Security Platform Vault node to an existing HSM configuration depends on whether you are using a single cluster certificate or individual node certificates.

In both cases, though, you should deploy the node as usual and then join it to the existing cluster. For details on adding an already-deployed node, see Joining or Re-joining a CSP Vault Cluster. For details on deploying a new node,

Single Cluster Certificate

If you are using a single cluster certificate, you do not need to do anything special to connect the new node to your existing HSM configuration. Cryptographic Security Platform Vault automatically adds to the new node to your existing HSM configuration when you add it to the cluster.

This is true for both single HSM and multiple HSM configurations.

Individual Node Certificates

Before You Begin

For *each* hardware security module (HSM) that is currently connected to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password for the partition to which the existing Cryptographic Security Platform Vault clients have been assigned.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM servers via a shell account. The following procedure uses `ssh` to connect to the servers.

Note: The following instructions are specific to the Luna HSM.

Procedure

If you are using individual node certificates, you need to do the following after you have added the new node to the cluster:

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.

5. Navigate to the **Client List** tab. You should see one entry for each Cryptographic Security Platform Vault node in the cluster.
6. Select the new node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called *node-name.domain-name*.pem and downloads it to your browser's default download location.
   For example, if the name of the node is KC-4 and it is running on the domain my-company.com, the certificate file would be called KC-4.my-company.com.pem.
7. Upload the node certificate to the root directory on each HSM server that you want to use. For example, if you have two HSM servers, you would copy the new node certificate to both HSM servers:
   ```
   # scp KC-4.my-company.com.pem admin@hsm1.my-company.com:
   admin@hsm1.my-company.com's password:

   KC-4.my-company.com.pem          100% 1164     1.1KB/s   00:00

   # scp KC-4.my-company.com.pem admin@hsm2.my-company.com:
   admin@hsm2.my-company.com's password:

   KC-4.my-company.com.pem          100% 1164     1.1KB/s   00:00
   ```
8. Using a shell account, log into each HSM server and:
   a. Register the new Cryptographic Security Platform Vault client using "*node-name.domain-name*" for both the client name and hostname. The double quotes are required because of the period in the client name.
      Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the name of the client pem file that Cryptographic Security Platform Vault generates.
   b. Assign a partition to the Cryptographic Security Platform Vault client.

   For example, if you want the Cryptographic Security Platform Vault client KC-4.my.company.com to be assigned to KC_partition1 on hsm1.my-company.com and to KC_partition2 on hsm2.my-company.com, you could enter:
   ```
   # ssh admin@hsm1.my-company.com
   admin@hsm1.my-company.com's password:

   [hsm1] lunash:>client register -client "KC-4.my-company.com" -hostname "KC-4.my-company.com"

   'client register' successful
   Command Result : 0 (Success)
   [hsm1] lunash:>client assignPartition -client "KC-4.my-company.com" -partition KC_partition1
   'client assignPartition' successful
   Command Result : 0 (Success)
   [hsm1] lunash:>exit

   # ssh admin@hsm2.my-company.com
   admin@hsm2.my-company.com's password:

   [hsm2] lunash:>client register -client "KC-4.my-company.com" -hostname "KC-4.my-company.com"

   'client register' successful
   Command Result : 0 (Success)
   [hsm2] lunash:>client assignPartition -client "KC-4.my-company.com" -partition KC_partition1
   'client assignPartition' successful
   ```

```
Command Result : 0 (Success)
[hsm2] lunash:>exit
```

9. If you want to verify the connection, return to the Cryptographic Security Platform Vault webGUI and navigate to the **Server Settings** tab, then click **Test**. You should see a message that says the HSM connection is OK.

Adding a New Luna HSM to an Existing Luna HSM Configuration

If you have already configured your Cryptographic Security Platform Vault cluster to use a Luna hardware security module (HSM) server, you can add a new Luna HSM server to your configuration at any time. Adding additional HSM servers and configuring an HA Group provides High Availability (HA) if one HSM server should become unreachable.

The following procedure describes how to add an additional Luna HSM when you have already configured one or more Luna HSMs. If you only have a Luna Cloud HSM configured, see Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate or Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates. If this is the first time you are configuring an HSM server for your Cryptographic Security Platform Vault cluster, see Hardware Security Modules with CSP Vault.

Before You Begin

For the new HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and partition password. We recommend that you use a different partition name on each HSM server so that you can tell the servers apart when you are working with the HA group.
  Note: Luna requires that the partition password be the same on all servers in an HA group, and that certain configuration options be the same on all HSM servers in the group. For details, see your Luna HSM documentation.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the new HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

Note: The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the new HSM server. We recommend that you rename the `server.pem` certificate file so that you know which HSM server goes with which certificate file.
   For example, if the new HSM server is `hsm2.my-company.com`, you could enter:
   ```
   # scp admin@hsm2.my-company.com:server.pem ./hsm2cert.pem
   admin@hsm2.my-company.com's password:

   server.pem          100% 1155     1.1KB/s   00:00
   ```
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.

6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the **Luna HSM Server Settings** tab, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.
    a. Change the **Hostname** to the name of the new HSM server.
    b. Change the **Partition Label or HA Group Name** to the partition that Cryptographic Security Platform Vault should use on the new HSM server. We recommend that you use a different partition name on each server so that you can tell which server is which when you are creating the Luna HA group later in this procedure.
    c. In the **Server Certificate** field, click **Browse** and select the server certificate for this HSM server.
    d. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.

    Note: Because Luna requires that all HSM servers in a High Availability group have the same password, you do not need to enter the password for any additional HSM servers. Cryptographic Security Platform Vault automatically uses the most recent password entered for all servers in the group.
8. If you do not have the original Cryptographic Security Platform Vault client cluster certificate or node certificates, you need to regenerate them. How you do so depends on the selected **Client Mode**.

Client Mode Setting	Steps to Regenerate the Certificates
CLUSTER	Select Actions > Generate Client Certificate. Cryptographic Security Platform Vault automatically saves *client-name*.pem file to your browser's default download location.
NODE	a. Navigate to the **Client List** tab. b. Select the first node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called *node-name.domain-name*.pem and downloads it to your browser's default download location. c. Repeat step 2 for each node in the cluster until you have a full set of node certificates.

    Note: If you regenerate the cluster certificate or node certificates you must upload the new certificate(s) to all the Luna HSM servers.
9. Upload the cluster certificate or the individual node certificates to the root directory on the new HSM server.
    Cluster Mode Example
    If your Cryptographic Security Platform Vault cluster name is KC_Cluster and the new HSM server is hsm2.my-company.com, you would enter:

```
# scp KC_Cluster.pem admin@hsm2.my-company.com:
admin@hsm2.my-company.com's password:

KC_Cluster.pem          100% 1164     1.1KB/s   00:00
```

    Node Mode Example
    If you have two Cryptographic Security Platform Vault nodes named KC-1 and KC-2 and the new HSM server is hsm2.my-company.com, you would enter:

```
# scp KC-1.my-company.com.pem admin@hsm2.my-company.com:
admin@hsm2.my-company.com's password:

KC-1.my-company.com.pem          100% 1164     1.1KB/s   00:00
```

```
# scp KC-2.my-company.com.pem admin@hsm2.my-company.com:
admin@hsm2.my-company.com's password:

KC-2.my-company.com.pem          100% 1164     1.1KB/s   00:00
```

10. Using a shell account, log into the new HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using the client name for both the client name and hostname parameters. Use double quotes if the client name includes any periods or spaces.
    Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the client name after the initial HSM configuration has been completed.
    b. Assign any partitions that you intend to use to the Cryptographic Security Platform Vault client.
    Note: This should include the partition specified above, and any others that you intend to use from Vaults.

    Cluster Mode Example

    For example, if you want the Cryptographic Security Platform Vault client `KC_Cluster` to be assigned to `KC_partition2` on `hsm2.my-company.com`, you could enter:

```
# ssh admin@hsm2.my-company.com
admin@hsm2.my-company.com's password:

[hsm2] lunash:>client register -client KC_Cluster -hostname KC_Cluster
'client register' successful
Command Result : 0 (Success)
[hsm2] lunash:>client assignPartition -client KC_Cluster -partition KC_partition1
'client assignPartition' successful
Command Result : 0 (Success)
[hsm2] lunash:>exit
```

    Node Mode Example

    For example, if you want the Cryptographic Security Platform Vault clients `KC-1` and `KC-2` to be assigned to `KC_partition2` on `hsm2.my-company.com`, you could enter:

```
# ssh admin@hsm2.my-company.com
admin@hsm2.my-company.com's password:

[hsm2] lunash:>client register -client "KC-1.my-company.com" -hostname "KC-1.my-
company.com"
'client register' successful
Command Result : 0 (Success)
[hsm2] lunash:>client register -client "KC-2.my-company.com" -hostname "KC-2.my-company.com"

'client register' successful
Command Result : 0 (Success)
[hsm2] lunash:>client assignPartition -client "KC-1.my-company.com" -partition KC_partition3
'client assignPartition' successful
Command Result : 0 (Success)
[hsm2] lunash:>client assignPartition -client "KC-2.my-company.com" -partition KC_partition3
'client assignPartition' successful
Command Result : 0 (Success)
```

11. Repeat this procedure for any more Luna HSMs that you wish to add. If you wish to add a Luna Cloud HSM, see Adding a Luna Cloud HSM to an Existing Luna HSM Configuration.

After you have configured all the Luna HSM servers and optionally a Luna Cloud HSM, create a Luna HSM HA group that links the HSM servers together so that all keys will be saved to all servers in the group. For details, see Configuring a Luna HSM HA Group.

Adding a Luna Cloud HSM to an Existing Luna HSM Configuration

If you have already configured your Cryptographic Security Platform Vault cluster to use one or more Luna hardware security module (HSM) serverx, you can add a Luna Cloud HSM server to your configuration. You can then configure an HA Group or add it to the existing HA Group. This provides High Availability (HA) if one HSM server should become unreachable. For more information, see Configuring a Luna HSM HA Group.

You can only have a single Luna Cloud HSM configured. If you also have any Luna HSMs, you must configure an HA Group and specify the same HA Group in both the Luna HSM and Luna Cloud HSM tabs of the Luna HSM Server Settings page.

Follow the instructions at Configuring CSP Vault as a Luna Cloud HSM Client to add the Luna Cloud HSM, and then use the instructions at Configuring a Luna HSM HA Group to create and select the HA Group.

Note: The partition that you use on the Luna Cloud HSM must use the same password as those on the Luna HSMs and meet the other requirements for membership in an HA group. For details about these requirements, see your Luna HSM documentation.

Changing the Luna Client Certificate Mode

If you have an existing Luna HSM configuration and you want to change from using a single cluster certificate to individual node certificates, or if you want to change from individual node certificates to a single cluster certificate, you need to reset your HSM configuration and recreate it from the beginning.

Warning:

- When you reset your HSM configuration, Cryptographic Security Platform Vault permanently deletes all Admin keys stored on any HSM servers in the current configuration. It then generates a new Admin Key. Make sure you download this Admin Key and keep it securely in case you need to restore your CSP Vault system to its current state. After reconfiguring the HSM settings you can generate a new Admin Key stored in the HSM(s).
- If any of your Cloud VM Sets use a KEK (Key Encryption Key) , the KEKs will *not* be deleted. However, Cryptographic Security Platform Vault will not be able to access those KEKs until you reconfigure the connection to the same partition on at least one of the HSM servers that you originally used. If a VM protected by a KEK is rebooted before the HSM server connection had been reestablished, the reboot will fail and VM will not be accessible to any users. For more information, see KEKs with Cloud VM Sets.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Click **Reset Server Settings** and confirm the reset at the prompt.
6. Reconfigure your HSM settings as described in Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate or Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates.

Locating the HSM Server Admin Key

If your Admin key is stored in the HSM, you can use Cryptographic Security Platform Vault to locate it.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. In the Admin Key ID field, click **Locate Admin Key**.
   The location of the Admin key ID is displayed at the bottom of the page.

Resetting the HSM Server Configuration

When you reset your HSM configuration, keep the following in mind:

- Cryptographic Security Platform Vault permanently deletes all Admin keys stored on any HSM servers in the current configuration. It then generates a new Admin key. Make sure you download this Admin Key and keep it securely in case you need to restore your Cryptographic Security Platform Vaultsystem to its current state.
- If you are using Luna HSMs or Luna Cloud HSMs:
  - If any of your Cloud VM Sets use a KEK (Key Encryption Key) , the KEKs will *not* be deleted. However, Cryptographic Security Platform Vault will not be able to access those KEKs until you reconfigure the connection to the same partition on at least one of the HSM servers that you originally used. If a VM protected by a KEK is rebooted before the HSM server connection had been reestablished, the reboot will fail and VM will not be accessible to any users. For more information, see KEKs with Cloud VM Sets.
    Important: You must disable the KEK setting in every Cryptographic Security Platform Vault for KMIP before you reset the HSM.
  - The Cryptographic Security Platform Vault client on the Luna HSM servers will not be deleted. If you want to remove the Cryptographic Security Platform Vault client from the Luna HSM server, you must do this manually on each Luna HSM server in your configuration.
- If you are using *both* Luna HSMs and Luna Cloud HSMs you must reset both HSMs.
- If you are using nShield HSMs:
  - All keys will be deleted. You should disconnect all CSP Vaults from the HSM before resetting the HSM configuration.
  - If you have enabled HSM Root-of-Trust, you cannot reset the HSM server configuration.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Reset the server as follows:
   - For nShield, select **Actions > Reset HSM Configuration**.
   - For Luna HSM, select **Actions > Reset Luna HSM Configuration**.
   - For Luna Cloud HSM, select **Actions > Reset Luna Cloud HSM Configuration**.
6. Confirm the reset at the prompt.

SNMP Traps in Cryptographic Security Platform Vault

You can configure Cryptographic Security Platform Vault to send an SNMP (Simple Network Management Protocol) trap whenever an alert is generated. These alerts can be divided into two categories:

- System-level alerts apply to events that are handled by Security Admins, such as numerous failed login attempts for a Cryptographic Security Platform Vault user account or if the Cryptographic Security Platform Vault license is about to expire.

- Group-level alerts apply to events that are handled by Cloud Admins or Domain Admins, such as if a VM needs to be re-authorized or if the Cryptographic Security Platform Vault cluster status changes.

You can specify one system-level SNMP trap configuration and one group-level SNMP trap configuration for each Cloud Admin or Domain Admin user group in the system.

If a group-level alert is raised and there is no matching group-level SNMP trap configuration, Cryptographic Security Platform Vault defaults to the system-level SNMP trap configuration.

This section includes:

Configuring Group-Level SNMP Traps

The group-level trap configurations are used for alerts that affect Cloud Admins or Domain Admins. If no group-level configuration is specified for a particular group-level alert, Cryptographic Security Platform Vault defaults to the System-level SNMP configuration settings.

1. Log into the Cryptographic Security Platform Vault webGUI on any node in the cluster using an account with the security privilege that matches the type of group configuration you want to create. For example, if you want to create a Cloud Admin group-level SNMP configuration, you need to log in with Cloud Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Group Settings** section, click **Group SNMP Settings**.
4. On the SNMP Settings page, select the Cloud Admin Group to which you want the configuration to apply in the **Group** field.
5. Specify the SNMP configuration options you want to use.

Field	SNMP Version	Description
Enabled	All	Select True if you want Cryptographic Security Platform Vault to use this SNMP configuration.
Server	All	The hostname or IP address of the SNMP server.
Port	All	The SNMP port number. The default SNMP port is 162.
Version	All	The SNMP version. Cryptographic Security Platform Vault supports version 2c and version 3. Note: The rest of the fields displayed in page depend upon the selected version.
Community	2c	Specify the community string for your SNMP server.

Field	SNMP Version	Description
User	3	The user ID that should be associated with the trap.
Notification Type	3	This can be: • Inform—Cryptographic Security Platform Vault sends the SNMP trap and expects an acknowledgment that the trap was received in return. • Trap—Cryptographic Security Platform Vault sends the SNMP trap but does not expect an acknowledgment.
Engine ID Type	3	Choose the engine ID type from the following options: • Custom Engine ID—Choose this option if an SNMP engine ID is already configured in the SNMP Manager. This allows users to configure the same engine ID in the engine ID field. Cryptographic Security Platform Vault will send the traps with the supplied engine. • System Generated Engine ID—Choose this option if the SNMP Manager expects to receive the engine ID from the Cryptographic Security Platform Vault. The Engine ID field will be automatically filled with a system generated engine ID that cannot be edited. Updating the system generated engine ID may take a few minutes. Note: This field is only visible if the Notification Type is Trap.
Engine ID	3	If the Notification Type is Trap, enter the SNMP engine ID assigned to the SNMP manager. You can enter between 10 and 64 hexadecimal characters.

Field	SNMP Version	Description
Security Level	3	This can be: • **No Authentication, No Privacy** — Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy** — Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy** — Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.

6. When you are finished, click **Apply**.
7. If you want to test the configuration, click **Test SNMP Settings**.
   Note: The SNMP trap must be enabled and you must apply the settings before you can test the configuration.
8. If you want to download the MIB file, click **Download MIB File**.

Configuring SNMP Agent Users for Polling

After you enable SNMP traps, you can configure one or more SNMP agent users that allow the SNMP agent to poll Cryptographic Security Platform Vault for system information.

The following OIDS are available for querying:

- IF-MIB::ifTable (.1.3.6.1.2.1.2.2)
- HOST-RESOURCES-MIB::hrFSTable (.1.3.6.1.2.1.25.3.8)
- HOST-RESOURCES-MIB::hrSystem (.1.3.6.1.2.1.25.1)
- 'NET-SNMP-EXTEND-MIB::nsExtendOutputFull."svstat"' (.1.3.6.1.4.1.8072.1.3.2.3.1.2.6.115.118.115.116.97.116)
- SNMPv2-MIB::system (.1.3.6.1.2.1.1)
- UCD-SNMP-MIB::dskTable (.1.3.6.1.4.1.2021.10)
- UCD-SNMP-MIB::laTable (.1.3.6.1.4.1.2021.9)
- UCD-SNMP-MIB::memory (.1.3.6.1.4.1.2021.4)
- UCD-SNMP-MIB::systemStats (.1.3.6.1.4.1.2021.11)

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges. In the top right, click the Switch to **Appliance Management** link.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section click **SNMP Settings**.
4. Click the **Agent Users** tab.
5. To create a new agent, click **Actions > Add User** and specify the options you want to use. When you are done, click **Apply**.
   Note: SNMP agent settings cannot be changed after you save the agent.

Field	SNMP Version	Description
Version	All	The SNMP version. Cryptographic Security Platform Vault supports version 2c and version 3. Note: The rest of the fields displayed in page depend upon the selected version.
Network	2c	An optional field that restricts access to the specified IP address of a host or network. For example: 192.168.100.0/24.
Community	2c	The community string for your SNMP server.
User	3	The user ID that should be associated with the agent.

Field	SNMP Version	Description
Security Level	3	This can be: • **No Authentication, No Privacy**—Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy**—Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy**—Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.

6. To delete an existing agent, select that agent then select **Actions > Delete Selected User**. To delete multiple users, enable **Multi-Select**, click the agents you want to delete, then select **Actions > Delete Selected Users**.

Configuring System-Level SNMP Traps

The system-level trap configuration is always used for alerts that affect Security Admins. It is also used for group-level alerts if no specific group-level configuration exists in Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.

2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **SNMP Settings**.
5. On the SNMP Settings page, specify the options you want to use.

Field	SNMP Version	Description
Enabled	All	Select True if you want Cryptographic Security Platform Vault to use this SNMP configuration.
Server	All	The hostname or IP address of the SNMP server.
Port	All	The SNMP port number. The default SNMP port is 162.
Version	All	The SNMP version. Cryptographic Security Platform Vault supports version 2c and version 3. Note: The rest of the fields displayed in page depend upon the selected version.
Community	2c	Specify the community string for your SNMP server.
User	3	The user ID that should be associated with the trap.
Notification Type	3	This can be: • Inform—Cryptographic Security Platform Vault sends the SNMP trap and expects an acknowledgment that the trap was received in return. • Trap—Cryptographic Security Platform Vault sends the SNMP trap but does not expect an acknowledgment.

Field	SNMP Version	Description
Engine ID Type	3	Choose the engine ID type from the following options: • Custom Engine ID—Choose this option if an SNMP engine ID is already configured in the SNMP Manager. This allows users to configure the same engine ID in the engine ID field. Cryptographic Security Platform Vault will send the traps with the supplied engine. • System Generated Engine ID—Choose this option if the SNMP Manager expects to receive the engine ID from the Cryptographic Security Platform Vault. The Engine ID field will be automatically filled with a system generated engine ID that cannot be edited. Updating the system generated engine ID may take a few minutes. Note: This field is only visible if the Notification Type is Trap.
Engine ID	3	If the Notification Type is Trap, enter the SNMP engine ID assigned to the SNMP manager. You can enter between 10 and 64 hexadecimal characters.
Security Level	3	This can be: • **No Authentication, No Privacy** — Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy** — Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy** — Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).

Field	SNMP Version	Description
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Agent Port	All	The port to use for all SNMP Agent Users. The default is port 161.

6. When you are finished, click **Apply**.
7. If you want to test the configuration, click **Test SNMP Settings**.
   Note: The SNMP trap must be enabled and you must apply the settings before you can test the configuration.
8. If you want to download the MIB file, click **Download MIB File**.

Downloading the SNMP MIB File

1. Log into the Cryptographic Security Platform Vault webGUI on any node in the cluster using an account with Security Admin, Cloud Admin, or Domain Admin privileges.
2. In the top menu bar, click **Settings**.
3. If your user account has:
   - Security Admin privileges, click **SNMP Settings** in the **System Settings** section and select **Actions > Download MIB File**.
   - Domain Admin or Cloud Admin privileges, click **Group SNMP Settings** in the **Group Settings** section and click **Download MIB File** at the bottom of the SNMP Settings page.

   Cryptographic Security Platform Vault downloads `HTKC-MIB.txt` to your browser's default download location.
4. Import the MIB file into your SNMP trap receiver so that the Cryptographic Security Platform Vault traps are readable in your SNMP tool. For details, see your SNMP documentation.

SNMP MIB File

The SNMP MIB (Management Information Base) file defines the properties for the managed objects in Cryptographic Security Platform Vault. The MIB file is written in an independent format and the object information it contains is organized hierarchically. OIDs (Object Identifiers) in the MIB file uniquely identify each managed object. Each OID has an address that follows the levels of the OID hierarchy.

The Enterprise OID for HyTrust is 1.3.6.1.4.1.33095. Cryptographic Security Platform Vault's relative OID is 4.

Object Model

The model for a Cryptographic Security Platform Vault MIB trap object is:

```
-- 1.3.6.1.4.1.33095.4.1.0.1
htkcKeyServerAlert NOTIFICATION-TYPE
    OBJECTS     { htkcKeyServerAlertID, htkcKeyServerAlertSeverity, htkcKeyServerAlertText,
htkcKeyServerHostname, htkcKeyServerIP, htkcDeviceHostname, htkcDeviceIP, htkcObjectName,
htkcObjectID, htkcObjectType, htkcObjectDetail }
    STATUS      current
    DESCRIPTION "An HTKC alert."
    ::= { htkcKeyServerAlerts 1 }
```

Message Fields

Message Field	Description
htkcKeyServerAlertID	The Alert ID number.
htkcKeyServerAlertSeverity	The alert severity. This can be 0 (high), 5 (medium), or 10 (low).
htkcKeyServerAlertText	The alert text.

Host Identification Fields

Field	Description
htkcKeyServerHostname	Hostname of the Cryptographic Security Platform Vault server generating the alert.
htkcKeyServerIP	IP address of the Cryptographic Security Platform Vault server generating the alert.
htkcDeviceHostname	Hostname of device for which alert is being generated. If the alert is about the Cryptographic Security Platform Vault cluster, this will be the same as `htkcKeyServerHostname`. If it is about a client object such as a VM, disk, or filesystem, this will be the hostname of the VM on which the Policy Agent is running.
htkcDeviceIP	The IP address of the device for which alert is being generated. This will either be the IP address of the Cryptographic Security Platform Vault server or the address of the client VM on which the Policy Agent is running.

Object Identification Fields

The following fields only apply if the object identity is available.

Field	Description
htkcObjectName	Name of object for which alert is being generated.

Field	Description
htkcObjectID	UUID of object for which alert is being generated.
htkcObjectType	Type of object for which alert is being generated.
htkcObjectDetail	JSON string containing hierarchical list of objects starting from leaf node. This is necessary for identifying the object based on name.

Example

For example, here is a sample trap for the alert stating that Virtual Machine dkw2012 has been authenticated. The alert ID is 85 and the priority is 10 (low).

2018-07-26 14:57:44 dkkc2 [UDP: [172.16.14.22]:19357->[0.0.0.0]:0]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::snmpTrapOID.0 = OID: HTKC-MIB::htkcKeyServerAlert
HTKC-MIB::htkcKeyServerAlertID = Gauge32: 85
HTKC-MIB::htkcKeyServerAlertSeverity = INTEGER: low(10)
HTKC-MIB::htkcKeyServerAlertText = STRING: "Added Virtual Machine dkw2012 (Cloud VM Set: windows), authentication complete"
HTKC-MIB::htkcKeyServerHostname = STRING: "dkkc2.localdomain"
HTKC-MIB::htkcKeyServerIP = STRING: "172.16.14.22"
HTKC-MIB::htkcDeviceHostname = "dkw2012.localdomain"
HTKC-MIB::htkcDeviceIP = STRING: "172.16.14.169"
HTKC-MIB::htkcObjectName = STRING: "dkw2012"
HTKC-MIB::htkcObjectID = STRING: "24bc7e36-90b6-11e8-a0fc-000c29cd584d"
HTKC-MIB::htkcObjectType = STRING: "CVM"
HTKC-MIB::htkcObjectDetail = STRING: "[{\"type\": \"CVM\", \"name\": \"dkw2012\", \"id\": \"24bc7e36-90b6-11e8-a0fc-000c29cd584d\"}, {\"type\": \"CVMSET\", \"name\": \"windows\", \"id\": \"307e83d2-90b2-11e8-a0fc-000c29cd584d\"}, {\"type\": \"GROUP\", \"name\": \"Cloud Admin Group\", \"id\": \"d2e6a25b-9096-11e8-a0fc-000c29cd584d\"}]"

Setting CSP Vault Management webGUI Alert Settings

The CSP Vault Management webGUI receives alerts for your CSP Vault managed user objects which can impact cluster performance. You can disable these alerts to improve performance.

Note: Disabling webGUI alerts does not affect SNMP or email alerts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **WebGUI Alert Settings**.
5. On the WebGUI Alert Settings page, select one of the following:
   - Select **Enable** if you want to receive webGUI alerts.
   - Select **Disable** if you do not want to receive webGUI alerts.
6. Click **Apply**.

Using the Entrust CSP Vault System Console

When you log into the Cryptographic Security Platform Vault VM console as `htadmin`, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. This menu lets you configure the local Cryptographic Security Platform Vault server. In general, the changes you make here do not apply to any other node in the cluster.

The menu is a TUI (Text-based User Interface). You navigate through the TUI using the Tab key to move between fields and pressing Enter when the correct choice is highlighted. If the TUI screen has numbers at the start of the line, you can also press the corresponding number key and then press Enter to navigate through the menus.

To return to the main Entrust Cryptographic Security Platform Vault System Console screen, press Esc (Escape). Based on where you are in the menus, you may need to press Esc several times.

The Entrust Cryptographic Security Platform Vault System Console contains the following options:

Option	Name	Description
1	Manage Network Settings	View or change the current network configuration. This menu also allows you to run network diagnostic tools. For details, see Troubleshooting Network Issues.
2	Manage htadmin and SSH Access	Manage the `htadmin` account for this Cryptographic Security Platform Vault node and enable or disable access to the Entrust Cryptographic Security Platform Vault System Console via SSH.
3	Manage Accounts	Enable or disable the full support login account (`htsupport`), the restricted login account (`htrestricted`), or the Cryptographic Security Platform Vault webGUI default account (secroot).
4	Manage HSM Client Account	If you are connecting Cryptographic Security Platform Vault to multiple HSM servers, this option allows you to configure those servers as an HA group. For details, see Hardware Security Modules with CSP Vault.
5	Download Entrust Internal Certificate	Download the Entrust-generated CA certificate being used on this Cryptographic Security Platform Vaultnode so that you can add that certificate to your web browser as a trusted site. For details, see CSP Vault Certificates.

Option	Name	Description
6	Gather Diagnostic Logs	Creates a support bundle with diagnostic information and log files that Entrust Support can use to diagnose issues with your Cryptographic Security Platform Vault cluster. To create a support bundle using the webGUI, see Creating a Support Bundle with the webGUI.
7	Manage CSP Vault Management Node	Allows you to delete internal snapshots created automatically during upgrade.
8	Reboot or Shut Down CSP Vault Management Node	Reboots or shuts down the current Cryptographic Security Platform Vault node. If you plan to remove the node from the cluster or decommission it, see Removing a CSP Vault Node from a Cluster or Decommissioning a CSP Vault Node.
9	Manage Timeouts and Appearance	View or change the current timeout for the Entrust Cryptographic Security Platform Vault System Console. After this period of time elapses with no user input, Cryptographic Security Platform Vault closes the Entrust Cryptographic Security Platform Vault System Console and returns to the system login prompt. This option also lets you toggle the 3D appearance for the Entrust Cryptographic Security Platform Vault System Console.
10	Quit TUI Session	Close the Entrust Cryptographic Security Platform Vault System Console and return to the system login prompt.

CSP Vault Authentication and User Accounts

There are two types of CSP Vault user accounts:

- Cryptographic Security Platform Vault-managed user accounts. These are individual accounts created and administered locally in Cryptographic Security Platform Vault. A Cryptographic Security Platform Vault-managed account can be authenticated locally (with a password stored in Cryptographic Security Platform Vault) or externally (with a password stored in an LDAP server), and it can have any combination of the available user roles: Security Admin, Domain Admin, and Cloud Admin. These three user roles and their privileges are described below.
  With Cryptographic Security Platform Vault-managed accounts, a Cryptographic Security Platform Vault Security Admin should create one user account for each person who needs access to Cryptographic Security Platform Vault, being careful to assign each account the appropriate user roles and access rights.
- Active Directory (AD)-managed user accounts. Unlike Cryptographic Security Platform Vault-managed accounts where you have to create one account for each Cryptographic Security Platform Vault user, AD-managed users are granted access at the AD Security group level. When a Cryptographic Security Platform Vault Security Admin creates a Cloud Admin Group, they can assign one or more AD Security groups to

that Cloud Admin Group. When they do so, every individual in every explicitly-named AD Security group is automatically granted Cloud Admin access to Cryptographic Security Platform Vault. (For more information, see Considerations When Using AD Security Groups.)
AD Security groups can only be associated with a Cloud Admin Group, and the only available user role for an AD-managed user account is Cloud Admin. This means you cannot use an AD group to specify users that need Security Admin or Domain Admin access to Cryptographic Security Platform Vault. Those users must have their own Cryptographic Security Platform Vault-managed user account.

By default, the Cryptographic Security Platform Vault installer creates the Cryptographic Security Platform Vault-managed user account `secroot`, which is automatically assigned all three user roles and placed in the default Cloud Admin Group. You can change the password and group membership for `secroot`, but you cannot delete the account or change its assigned Security Admin user role. We recommend you only give the `secroot` password to a very small number of administrators who need root-level access. If you need to change the `secroot` password, see Resetting the secroot Account Password.

User Roles and Privileges

Security Admin

- Can manage the Cryptographic Security Platform Vault license.
- Can create or delete Cryptographic Security Platform Vault-managed user accounts and Cloud Admin Groups.
- Can specify the LDAP server that Cryptographic Security Platform Vault will use to authenticate AD user accounts.
- Can assign Cryptographic Security Platform Vault-managed users or AD groups to Cloud Admin Groups.
- Can manage the master Admin key and set up KMIP or HSM as a external key server.
- Can back up, restore, and upgrade Cryptographic Security Platform Vault.
- Can manage the Cryptographic Security Platform Vault KMIP server settings, accounts, and objects.
- Can enable Cryptographic Security Platform Vault features such as email settings and BoundaryControl.
- Can view all audit records. These records can be exported to an external syslog server.
- Can view and delete alerts.
- *Cannot* view any policies or virtual machines, and cannot modify any associated settings.

Domain Admin

- Can manage Entrust Cryptographic Security Platform Vault clusters by adding, removing, and authorizing Cryptographic Security Platform Vault nodes.
- Can configure Cryptographic Security Platform Vault node settings such as Cryptographic Security Platform Vault heartbeat.
- Can view audit log records and alerts generated by Domain Admin actions.

Cloud Admin

- Can manage the encryption of virtual machines that have the Entrust Policy Agent installed.
- Can create and manage Cloud VM Sets, which separate the encrypted VMs into logical groups such as "VMs running in AWS" or "UK Data Center VMs". The configuration settings selected for a Cloud VM Set are automatically applied to all VMs in that set.
- Can set options for specific VMs that override the default options specified in the Cloud VM Set.
- Can create certificates for VMs and specify key expiration dates.
- Can revoke access to individual encrypted disks/filesystems, or the whole VM. When access to disks is revoked, filesystems are forcibly unmounted, thus removing access to clear-text data.
- Can create encryption keys to securely move encrypted data between specified VMs in the same Cloud VM Set.
- Can view audit records and alerts generated from the all VMs in the Cloud VM Sets to which they have access.

This section includes:

Authentication for CSP Vault User Accounts

Cryptographic Security Platform Vault-Managed Account Authentication

Cryptographic Security Platform Vault-managed accounts can be authenticated locally, with a password stored in the Cryptographic Security Platform Vault Management webGUI. Security Admins can configure the password requirements and expiration options, as well as the maximum number of login attempts that are allowed before the user account is disabled and an expiration date after which the account will be automatically disabled.

- Locally, with a password stored in Cryptographic Security Platform Vault. Cryptographic Security Platform Vault Security Admins can configure the password requirements and expiration options, as well as the maximum number of login attempts that are allowed before the Cryptographic Security Platform Vault account is disabled and an expiration date after which the account will be automatically disabled.
- Externally, through a LDAP/Active Directory authentication server. Security Admins cannot change the password requirements or expiration options, but they can set the maximum number of login attempts that are allowed before the Cryptographic Security Platform Vault-managed account is disabled and they can set an expiration date on the account itself so that it cannot be used after a certain date.
  For LDAP and Active Directory servers, Security Admins can specify one and only one domain for all user account authentication. You can, however, configure multiple domain controllers to provide failover in case one controller becomes unreachable.
- Cryptographic Security Platform Vault also supports user authentication through an OpenID Connect provider. If a provider is configured, the Cryptographic Security Platform Vault login dialog contains not only the **Sign In** button but also a configurable button to start the authentication process using the provider. When the user has been authenticated via the OpenID Connect provider, the same username is used to obtain the LDAP permissions to Cryptographic Security Platform Vault.

Active Directory-Managed Account Authentication

Cryptographic Security Platform Vault requires customers to provide a service account in Active Directory settings. The service account is used for retrieving the list of AD objects to help Security Administrators configure members in KeyControl Groups. The service account configured in Active Directory settings requires the following read permissions in AD:

- User object: attributes distinguishedName, cn, sAMAccountName, userPrincipalName, mail
- Group object: attributes objectGUID, distinguishedName, cn, sAMAccountName

All Active Directory (AD)-managed accounts must belong to AD Security groups that are defined in the same AD domain. While you can specify multiple domain controllers to provide failover, all of the Security groups you want to use must be part of the same domain.

> Note: An AD-managed user account *cannot* log into Cryptographic Security Platform Vault for the first time if the Cryptographic Security Platform Vault cluster is degraded. AD accounts that have already successfully logged in at least once will continue to work, but, in a degraded state, Cryptographic Security Platform Vault cannot process a new AD user login.

If you plan to use a mix of Cryptographic Security Platform Vault-managed user accounts that are authenticated through LDAP along with AD Security groups, you must use the same AD domain for both the Cryptographic Security Platform Vault-managed accounts and the AD Security groups.

Configuring Local Authentication Settings

This procedure describes how to configure the password and account security options for all locally-authenticated Cryptographic Security Platform Vault-managed user accounts. Password requirements for externally-authenticated accounts is managed in your LDAP authentication server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **Local (Password)**.
6. On the **Basic** tab, change the options as desired, then click **Apply** when finished.

Field	Description
Password Expiration	The maximum number of days that a password can be used before it expires. Cryptographic Security Platform Vault also uses this value to calculate the default password expiration date when a new local Cryptographic Security Platform Vault user is created. (Default: 60.) Once a password expires, the user is prompted to change their account password the next them they log into the webGUI.
Max Failed Logins	The number of failed login attempts allowed before the user account is locked. (Default: 5.) If the maximum number of logins is exceeded, the next time the user attempts to log in they receive a message informing them that the account is disabled and telling them to talk to a Security Administrator. The Security Administrator must then re-enable the account as described in Re-enabling a CSP Vault-Managed User Account. Note: This option applies to all Cryptographic Security Platform Vault-managed accounts, even ones that are authenticated using LDAP.
Minimum Previous Passwords	The number of unique new passwords that must be associated with a user account before an old password can be used. (Default: 5.)

7. On the **Strength** tab, click the desired value to change the setting, then click **Save** when finished. If you change one of these settings, Cryptographic Security Platform Vault applies the new requirements to any new passwords created for a Cryptographic Security Platform Vault account. It does *not* apply the requirements to any existing Cryptographic Security Platform Vault account passwords.

Field	Description
Minimum Password Length	The minimum number of characters that must be in a password. (Default: 8.)
Minimum Uppercase Characters	The minimum number of characters that must be upper case. (Default: 1.)
Minimum Special Characters	The minimum number of characters that must be something other than a-z, A-Z,or 0-9. (Default: 1.)
Minimum Lowercase Characters	The minimum number of characters that must be lowercase. (Default: 1.)
Minimum Required Digits	The minimum number of characters that must be numeric. (Default: 1.)

8. When you are finished, click **Close**.

Specifying an LDAP/AD Authentication Server

For Cryptographic Security Platform Vault-managed user accounts, you can use any LDAP server. If you want to specify AD-managed Security groups whose members will have Cloud Admin access to the VMs registered with Cryptographic Security Platform Vault, you must specify a Windows Active Directory (AD) server.

Cryptographic Security Platform Vault uses the same settings for both local account authentication and AD Security group authentication. You can specify up to two AD domain controllers for failover, but both controllers must manage the same AD domain.

For OpenLDAP, see Specifying an OpenLDAP Authentication Server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **LDAP**.
6. On the **Domain** tab, specify the options you want to use. When you are done, click **Apply**.

Field	Description
Domain Name	The Domain name to use for account authentication. You cannot specify multiple domain names.
Directory Service Type	If you plan to use Microsoft AD directory services, then select Microsoft AD. Select OpenLDAP for all non-Microsoft AD directory services.
Service Account	The AD account that Cryptographic Security Platform Vault should use when logging into the AD server. Specify the account using one of the following formats: • Distinguished Name (DN). For example, `CN=Administrator,CN=users,DC=<company-name>,DC=com` • User Principal Name (UPN). For example, `administrator@<company-name>.com`. • Account username. For example, `administrator`. The AD account is usually an administrative user and it can have read only permissions on the AD server.
Service Account Password	The password for the Service Account.
UID Attribute	The Security Manager Account Name (sAMAccountName) for the user. This is the attribute of the user or group object that would be queried during search.

7. If you want to add or change a Domain Controller, go to the **Domain Controllers** tab. To add a controller, click the blue **+** (Plus) sign. You can add up to two domain controllers per Cryptographic Security Platform Vault cluster.
   If you specify two domain controllers, make sure your primary controller appears first in this list. Cryptographic Security Platform Vault always tries to authenticate an AD user through the first domain controller listed.
   To edit an existing domain controller, select that controller and then click the edit button. You can specify the following basic options:

Field	Description
Server URL	The LDAP server IP address or hostname. Select `ldap://` or `ldaps://` from the drop-down list and enter the URL in the text field. To include a port number, specify `:port` after the name. For example, `ldaps://10.238.66.33:389`.

Field	Description
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the LDAP server. Note: This option is only available if the Server URL starts with `ldap://`.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. Cryptographic Security Platform Vault uses the CA certificate to verify the SSL certificate used by the LDAP server/Active Directory. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. If you are using `ldaps://` or have selected the STARTTLS option for `ldap://`, click Load File and select the CA (Certificate Authority) certificate for the LDAP server.
User Search Context	The Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context	The Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.
Timeout	If multiple domain controllers have been specified, this is the amount of time Cryptographic Security Platform Vault should wait for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does *not* apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. When you are finished, click **Save & Close**. Cryptographic Security Platform Vault automatically verifies that it can reach the specified domain controller using the service account credentials you specified on the **Domain** tab.

Specifying an OpenLDAP Authentication Server

You can now use OpenLDAP for Cryptographic Security Platform Vault-managed user accounts.

For Microsoft AD services, see Specifying an LDAP/AD Authentication Server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **LDAP**.
6. On the **Domain** tab, specify the options you want to use. When you are done, click **Apply**.

Field	Description
Domain Name	The Domain name to use for account authentication. You cannot specify multiple domain names.
Directory Service Type	Select OpenLDAP.
Service Account	The service account that Cryptographic Security Platform Vault should use when logging into the OpenLDAP server. We recommend that you specify the account using the following format: `<CN>@<DOMAIN NAME>` Important: OpenLDAP does not support the UPN parameter. Using the `<CN>@<DOMAIN NAME>` format allows you to import OpenLDAP users correctly into the provider's database. The users can then authenticate with the provider in Cryptographic Security Platform Vault.
Service Account Password	The password for the Service Account.
UID Attribute	The Security Manager Account Name (sAMAccountName) for the user.

7. If you want to add or change a Domain Controller, go to the **Domain Controllers** tab. To add a controller, click the blue **+** (Plus) sign. You can add up to two domain controllers per Cryptographic Security Platform Vault cluster.
   If you specify two domain controllers, make sure your primary controller appears first in this list.
   To edit an existing domain controller, select that controller and then click the edit button. You can specify the following basic options:

Field	Description
Server URL	The LDAP server IP address or hostname. Select `ldap://` or `ldaps://` from the drop-down list and enter the URL in the text field. To include a port number, specify `:port` after the name. For example, `ldaps://10.238.66.33:389`.
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the LDAP server. Note: This option is only available if the Server URL starts with `ldap://`.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. Cryptographic Security Platform Vault uses the CA certificate to verify the SSL certificate used by the LDAP server/Active Directory. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. If you are using `ldaps://` or have selected the STARTTLS option for `ldap://`, click Load File and select the CA (Certificate Authority) certificate for the LDAP server.

If you want to specify advanced domain controller options, click **Show Advanced Settings** and specify the options you want to use.

Field	Description
User Search Context	The Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through OpenLDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context	The Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.

Field	Description
Timeout	If multiple domain controllers have been specified, this is the amount of time Cryptographic Security Platform Vault should wait for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does *not* apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. When you are finished, click **Save & Close**. Cryptographic Security Platform Vault automatically verifies that it can reach the specified domain controller using the service account credentials you specified on the **Domain** tab.

Configuring OIDC with Active Directory for CSP Vault

By default the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required.

This topic explains how to configure OIDC authentication.

Active Directory authentication is a prerequisite for OIDC. Ensure Active Directory Authentication is configured for the vault before configuring OIDC. See Specifying an LDAP/AD Authentication Server. For OpenID Connect login to be successful across all vaults, you must provide AD/OpenLDAP service credentials, and the credentials must be active.

Each vault can be configured with a separate OIDC server or a separate application from same server.

For an example of how to configure an OIDC provider, see Example: Configuring Entrust Identity as a Service. If you are using a cluster, even though you configure OIDC for only one node, you will need to enter the Callback URIs (the Login Redirect URIs and Logout Redirect URIs) for all nodes in the cluster.

Important: OIDC with AD is a legacy authentication mode that relies on Active Directory (AD) where the OIDC provider manages authentication and Active Directory manages identity. This option should be used only for existing OIDC configurations that are already integrated with AD. If you are not using AD, we recommend that you use OIDC without AD as your OIDC authentication method.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect (with LDAP)**.
6. Specify the OpenID Connect Configuration settings:

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Field	Description
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

7. Click **Browse** to upload the CA Certificate.
   Note: The certificate needs to be in base64 encoded pem format.
8. Click **Apply**.
   A dialog box displays the configuration.
9. Click **Verify and Enable**.
10. After the verification, ensure the OpenID Connector Configuration Status is set to **Enabled**.
11. The vault is now set for OIDC authentication.

Configuring OIDC for Cryptographic Security Platform Vault

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

> Note: If you want to use OIDC without AD, you can only change to that mode from the local authentication mode. If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

For an example of how to configure an OIDC provider, see Example: Configuring Entrust Identity as a Service. If you are using a cluster, even though you configure OIDC for only one node, you will need to enter the Callback URIs (the Login Redirect URIs and Logout Redirect URIs) for all nodes in the cluster.

Important: OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

7. Optional. Click **Browse** to upload the CA Certificate.
   Note: The certificate needs to be in base64 encoded pem format.
8. Enter the Admin Name and Admin Email for OIDC user.
   This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**.
   The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**.
    The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Configuring an OpenID Connect Provider

Cryptographic Security Platform Vault supports user authentication through an OpenID Connect provider. If a provider is configured, the Cryptographic Security Platform Vault login dialog contains not only the Cryptographic Security Platform Vault Sign In button but also a configurable button to start the authentication process using the provider.

Important:

- For OpenID Connect login to be successful across all vaults, you must provide AD/OpenLDAP service credentials, and the credentials must be active.
- When the user has been authenticated via the OpenID Connect provider, the same username is used to obtain the LDAP permissions to Cryptographic Security Platform Vault. Therefore, the User Principal Name (UPN) used for the OpenID Connect provider must match a configured user on the LDAP server.
- OpenLDAP does not support the UPN parameter. This might cause problems because the OpenID Connect provider might be unable to authenticate users if it cannot return a valid UPN. **Workaround**: Set the `sn` field in the OpenLDAP server to the UPN for the registered user. This allows you to import OpenLDAP users correctly into the provider's database. The users can then authenticate with the provider in Cryptographic Security Platform Vault.

Before You Begin

The OpenID Connect provider must be configured to accept the Cryptographic Security Platform Vault URLs. Each login dialog requires both a login and a logout URL, so for Cryptographic Security Platform Vault, you have to configure 2 URLs for each node in the cluster. You have to configure the login and logout URL for Cryptographic Security Platform Vault, these 2 URLs are also sufficient for all types of vaults.

In the following example of URL list for OpenID Connect provider, `KC_IP` is the hostname or IP address of the Cryptographic Security Platform Vault agent:

<https://KC_IP/v5/oidc/callback>
<https://KC_IP/v5/kc/oidc/logout>

From Cryptographic Security Platform Vault 10.1.1, the Cryptographic Security Platform Vault appliance and the various types of vaults support multiple IDP servers. Each vault can have a separate IDP configured or can have different applications of same IDP configured for OIDC authentication.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Type** drop-down list, select **OpenID Connect**.

Specify the options you want to use. When you are done, click Apply.

Field	Description
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs. Only one global OIDC provider can be configured per Cryptographic Security Platform Vault cluster. The same button appears and the same OIDC authentication method is used on the login dialogs to Cryptographic Security Platform Vault, the Cryptographic Security Platform Vault for KMIP webGUI, and the Cryptographic Security Platform Vault for Secrets webGUI.

Setting the CSP Vault Management webGUI Session Timeout

By default, a Cryptographic Security Platform Vault Management webGUI session is logged out automatically after 30 minutes of inactivity. You can shorten the timeout but you cannot lengthen it.

> Note: If the user closes the browser without explicitly logging out from Cryptographic Security Platform Vault Management webGUI first, Cryptographic Security Platform Vault Management webGUI does not end the session until the session timeout is reached.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Session Timeout**.
4. Use the slider to set the desired value. You can set the timeout to be between 1 and 30 minutes.
5. Click **Apply** to save your changes.

Setting the Default Account Expiration

When you create a Cryptographic Security Platform Vault-managed user account, Cryptographic Security Platform Vault automatically assigns an account expiration date 365 days from the date the account is created. If you change this default, the expiration date for existing accounts is not changed. The new value is only applied to future accounts.

The default expiration date can also be overridden on an account by account basis when you create a new user account. For details, see Creating a New CSP Vault-Managed User Account.

> Note: This option applies only to Cryptographic Security Platform Vault-managed accounts. It does not apply to AD-managed user accounts. For details, see CSP Vault Authentication and User Accounts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **KeyControl Account**.
5. In the **Account Expires After** field, click the existing value and enter a number of days between 1 and 999. The default is 365 days.
6. Click **Save** and close the General Settings dialog box.

Creating a New CSP Vault-Managed User Account

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Users**.
3. Select **Actions > Create User**.
4. Enter the following information. All fields are required.

Field	Description
Full Name	The full name of the user associated with the account. This name is included on any audit log messages generated by that user's activity. Therefore, we recommend that you specify a unique full name for each Cryptographic Security Platform Vault user.

Field	Description
Email	If your system is configured to send email alerts, they will be sent to this email address. The alerts a user sees depends on their user role and group access.
Account Decay	The amount of time an account can stay enabled without logging in. The default and maximum value is 10 years from the last login date. If the user does not log in within that time period, Cryptographic Security Platform Vault automatically disables the account, but does not delete it. You will need to contact Entrust Support to re-enable the account.
Account Enabled	Check this box to have the account be available as soon as you create it. If you clear this check box, Cryptographic Security Platform Vault sets the account status to Disabled and you will need to manually enable it through the webGUI.

5. Click **Add**.
6. When you see the **User Successfully Added** message, click **Close**.

Setting webGUI User Preferences

The webGUI user account preferences are saved in Cryptographic Security Platform Vault so that your preferences are available even if you log in from a new location or using a different browser.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, open the **User Menu** by clicking the down arrow following your login name.
4. Select **User Preferences**.
5. On the **User Preferences** page, you can:
   - Select the page you want Cryptographic Security Platform Vault to display automatically whenever you log into the webGUI by selecting it in the **Default Landing Page** drop-down list. The pages available depend on the privileges associated with your user account.
   - Reset the initial landing page to the Entrust default by clicking the **Reset Initial Landing Page to Default** button. The default page depends on the privileges associated with your account.
   - Have Cryptographic Security Platform Vault remember your table column settings between sessions by checking the **Save Column Preferences** check box. This option is enabled by default.
   - Restore all default table settings and remove any customizations by clicking the **Reset All Grids to Default Configuration** button.
   - Change the webGUI skin by selecting a theme in the **Theme** drop-down list.
6. When you are done, click **Save Preferences**.

Changing Your CSP Vault User Account Settings

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   Note: AD-managed account users can view their account settings but they cannot change them.
2. In the top right, click the Switch to **Appliance Management** link.

3. Click **Settings**.
4. To change your account settings, click the contents of the appropriate field. Cryptographic Security Platform Vault-managed account users can change:
    - Full Name—Click the current name and enter the new information. When you are done, click **Save**. The full name can contain letters, digits, hyphens (-), or underscores (_).
      Note: The full name is associated with any audit log messages generated by the activity on this account. We recommend that every user be assigned a unique full name. Before you change this information consult your Cryptographic Security Platform Vault Administrator to make sure the full name you want to use is available.
    - Password—Click the **Change Password** button and enter your new password in the **Change Password** dialog box. When you are done, click **Update Password**. You can only change the password for a locally authenticated Cryptographic Security Platform Vault-managed user account. All other account passwords must be changed through the external LDAP, or Active Directory authentication server.
    - Email Address—Click the current email address and enter the new information. When you are done, click **Save**.
    - Send Alert Notifications—If this is set to **On**, any alert notifications are emailed to the address associated with the account. If it is **Off**, alert notifications can only be viewed in the webGUI.
    - Two-Factor Authentication—If this is set to **On**, you are required to have an authentication token when logging into the webGUI. If it is set to **Off**, you can log in using your standard username/password combination. For details and supported accounts, see About Two-Factor Authentication.

Setting the secroot Account Expiration

You can set an expiration for the Security Administrator (`secroot`) user account or set it to never expire.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Users**.
3. Select the Security Administrator (`secroot`) user account in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
4. In the Account Expiration field, choose one of the following:
    - **Never**—The `secroot` user account will never expire. This is the default.
    - **Choose a date**—The `secroot` user account will expire on the date that you set. Click **Apply** to save the date that you selected.

Resetting the secroot Account Password

The Cryptographic Security Platform Vault webGUI has a default Cryptographic Security Platform Vault-managed user account called secroot. If you do not remember the credentials of any Cryptographic Security Platform Vault user account with Security Administrator privilege, or if you are locked out of the Cryptographic Security Platform Vault webGUI, you can reset the secroot credentials with a temporary password. You can reset the password using one of the following methods:

- **Generate random password and send it via email to secroot**—Use this option to generate a random temporary password for the `secroot` user and securely send it to their email account that is registered in Cryptographic Security Platform Vault. The `secroot` user must have an email account configured in the Cryptographic Security Platform Vault webGUI and have access to email. We recommend that you use this option if secroot has email configured and has access to email.

- **Enter new temporary password for secroot**—Use this option to enter a temporary password. You can either pass it to the `secroot` user outside of Cryptographic Security Platform Vault, or email it to the `secroot` user directly from Cryptographic Security Platform Vault.

Note: If you have Two-Factor Authentication enabled configured for `secroot`, you will be provided an option to optionally reset the `secroot` user's Two-Factor Authentication state/secret.

Procedure

1. Log into the Cryptographic Security Platform Vault VM console as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts**.
3. In the Manage Accounts page, select **secroot (**Cryptographic Security Platform Vault webGUI **default account)**.
4. On the Cryptographic Security Platform Vault - Reset `secroot` Account page, choose the option that you want and complete the following:
   - To use Cryptographic Security Platform Vault to generate a random password and send it to the `secroot` user:
     i. Select **Generate random password and send it via email to secroot**.
     ii. On the Generate random password and send it via email to secroot page, optionally choose **Reset Two-Factor Authentication**.
     iii. Select **OK**.

     The `secroot` user will receive an email with the temporary password. When they log into the Cryptographic Security Platform Vault webGUI with the temporary password, they are immediately prompted to update the password.
   - To enter your own temporary password for `secroot`:
     i. Select **Enter new temporary password for secroot**.
     ii. On the Enter new temporary password for secroot page, optionally choose **Reset Two-Factor Authentication** and **Send Temporary password to secroot via email**.
     Note: If you choose to email the temporary password, the `secroot` user must have an email account configured in the Cryptographic Security Platform Vault webGUI and have access to emails.
     iii. Select **OK**.
     iv. Enter and confirm the temporary password.
     v. Select **OK**.
     vi. On the confirmation screen, select **OK**.

     When the `secroot` user receives the temporary password and logs into the Cryptographic Security Platform Vault webGUI, they are immediately prompted to update the password.

About Two-Factor Authentication

Two-factor authentication requires you to enter two forms of identification before you can access the Cryptographic Security Platform Vault Management webGUI. The first form is your standard username/password combination, and the second is a one-time password (OTP) generated by a authorization app. The OTP is appended to your existing password. Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend that you enable it in your remote authentication provider.

Two-factor authentication can now be enabled and enforced for all local Cryptographic Security Platform Vault Management webGUI users by the security administrator. Once enforced, all users will be prompted to use two-factor authentication to log in to the Cryptographic Security Platform Vault Management webGUI.

Cryptographic Security Platform Vault supports HMAC-based One Time Passwords (HOTP) and Time-based One-time Passwords (TOTP). HOTP uses an event-based algorithm, and passwords generated through this method are valid until the next event occurs. TOTP passwords are only available for a very short amount of time and are therefore more secure.

Important: We have seen instances where, if a QR code is used, the Microsoft Authenticator replaced the entries for the same username from different Cryptographic Security Platform Vault clusters . If you are planning to use Microsoft Authenticator for same usernames in different Cryptographic Security Platform Vault clusters, please manually type in the account name and secret key for the second and subsequent accounts rather than scanning the QR code, and make sure that each account name is different.

Enabling Two-Factor Authentication

Even if two-factor authentication is not enforced by the security administrator, individual Cryptographic Security Platform Vault Management webGUI users can enable it on their own system.

> Note: For security, the Cryptographic Security Platform Vault Sign In page does not prompt for the OTP.

Before You Begin

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use a TOTP application such as Google Authenticator or Microsoft Authenticator. These applications continually create passwords that are valid for 30 seconds. If the current password will expire before you can submit the login request, you need to wait for it to generate a new password and then you can use that to log in.
- For HOTP authentication, you can use a HOTP application such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in a second time you must click the Next button in the app to generate a new password.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box:
    a. Select the HOTP or TOTP radio button.
    b. Scan the generated bar code with your authorization app.
    c. Enter the six-digit verification code from your app in the dialog box.
    d. Click **Continue**. Cryptographic Security Platform Vault verifies that the code is correct and displays a message indicating success or failure. If the code is not correct, re-enter it.
    e. After the code has been accepted, click **Done**.
5. When you log into the Cryptographic Security Platform Vault webGUI, you will need to append a valid OTP to your standard account password on the Cryptographic Security Platform Vault Management webGUI Login Page. Do not add any characters or spaces between your account password and the one-time password

generated by your authorization app. In addition, if you are using TOTP, make sure the password will not expire before you submit the login request.
For example, if your password is XyZ123$, and your OTP is 32325, you would enter the following in the password field: XyZ123$32325.

Managing Two-Factor Authentication

System administrators can enforce two-factor authentication for all Cryptographic Security Platform Vault Management webGUI users.

Enforcing Global Two-Factor authentication:

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **ENFORCED**.
5. Click **Apply**.

Disabling Global Two-Factor Authentication:

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

Changing CSP Vault Account Details as a Security Administrator

This procedure is for Cryptographic Security Platform Vault-managed user accounts only. You cannot change the account details for any AD-managed user accounts. For details, see CSP Vault Authentication and User Accounts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Security**.
4. Click the **KeyControl Managed Users** tab.
5. Select the account you want to modify in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
6. Click the tab containing the information you want to change.
   Note: For a full description of all information in the tabs, see Creating a New CSP Vault-Managed User Account.
   - The full name, account status, account expiration, and email information is on the **User** tab.
     The **User** tab also lets you disable two-factor authentication for another user's account. If you do so, however, the user will need to re-enable it themselves. You cannot enable two-factor authentication for any other user's account. For more information, see About Two-Factor Authentication.
     Note: Beginning with 5.2, the security administrator can globally enforce two-factor authentication for all users. For more information, see Managing Two-Factor Authentication.
   - The authentication method and password, including the password expiration, for locally-authenticated accounts is on the **Authentication** tab.
   - The user role and group membership information is on the **Privileges and Groups** tab.
7. Click the field that you want to change and enter the new value in that field. When you are done, click **Save**. Your changes are immediately applied to the account.

Re-enabling a CSP Vault-Managed User Account

A Cryptographic Security Platform Vault-managed user account can become disabled for the following reasons:

- The number of consecutive unsuccessful login attempts has exceeded the value set for **Max Failed Logins**. For more information, see Configuring Local Authentication Settings.
- A Cryptographic Security Platform Vault Security Admin has manually disabled the account.
- The expiration date associated with the account has passed.
- The **Account Enabled** check box was not selected when the user account was created.

Important: If you cannot log into any Cryptographic Security Platform Vault accounts with Security Admin privileges, contact Entrust Support.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Security**.
4. Select the account you want to re-enable in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
5. In the **Account Status** field, click **Disabled**.
6. Check the **Enabled?** check box and click **Save**.
7. Verify the expiration date in the **Account Expiration** field.
8. To change the account password, click the **Authentication** tab then click **Change Password**.

Your changes take effect immediately.

CSP Vault Cluster Maintenance

CSP Vault Nodes and Clusters

When you install Cryptographic Security Platform Vault, the process creates a Cryptographic Security Platform Vault node that can operate singly or be joined with other Cryptographic Security Platform Vault nodes to form an active-active cluster. These nodes can be installed in different geographic locations, but they *must* be able to communicate with each other, with the Policy Agent installed on the encrypted servers associated with the cluster, and other nodes, for example KMIP, HTSV, or BYOK.

All Cryptographic Security Platform Vault nodes in a cluster share configuration settings, keys, and policy information. Changes made on one node are automatically synced to all nodes in the cluster through an encrypted object store. This provides a failover mechanism in case a Cryptographic Security Platform Vault node becomes unreachable.

The Cryptographic Security Platform Vault nodes constantly exchange heartbeats to verify that every node in the cluster is reachable. If all nodes respond to the heartbeats, the cluster is considered "healthy". If one or more nodes stop responding for a given length of time, the cluster is considered "degraded". If a cluster is

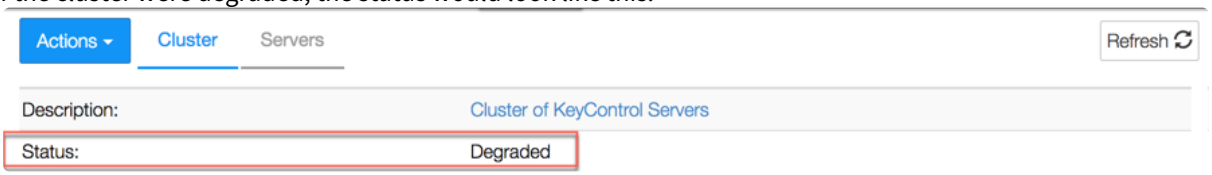
degraded, the active Cryptographic Security Platform Vault nodes can still serve requests for keys and policies from the associated Policy Agents, but you cannot make changes to the nodes in the cluster.

The heartbeat interval and status thresholds are user-configurable for the cluster. For details, see Setting Cluster Options.

Viewing the Cluster Status

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, look at the **Cluster** icon. If there is a green heart, the cluster is healthy. If there is a red X, the cluster is degraded. You can also look at the **Status** field on the **Cluster** tab.
   For example the following screenshot shows a healthy cluster containing two Cryptographic Security Platform Vault nodes.

   If the cluster were degraded, the status would look like this:



   Note: If the cluster is degraded, you cannot perform a backup.
4. To view the status of the individual servers in the cluster, click the **Servers** tab. The **Status** column shows the status for each server in the cluster:
   Maintenance—Same as cluster status, going through rolling upgrade.
   Offline—Unreachable and unavailable.
   Online—Reachable and available.
   Unavailable—Server to server connection (port 5432) works, but the KMIP Database is read-only.
   Unreachable—Unable to connect to the server (port 8443).
   Tip: To sort the unreachable servers to the top, click the Down Arrow (**v**) in the **Status** column and select **Sort Descending**.
5. A yellow star appears before the server name of the node that has been designated as the KMIP database master node. The other nodes in the cluster are replica nodes.
   All KMIP requests are forwarded to the master node for execution and when the master node's database is updated, all replica nodes receive the new updates synchronously.

Setting Cluster Options

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Specify the options that you want to use:

Option	Description
Description	A user-defined description for the cluster.
Status	The status of the cluster. If this is Healthy, all Cryptographic Security Platform Vault nodes are functioning normally. If this is Degraded, Cryptographic Security Platform Vault can still serve requests for keys and policies from the associated Policy Agents, but you cannot make changes to the nodes in the cluster.
Group Administrator	The Cryptographic Security Platform Vault administration group to which this cluster belongs. You cannot change this field.
Backup Hosts	The hostnames or IP addresses of systems that are allowed to access the Cryptographic Security Platform Vault backup directory through NFS. (`0.0.0.0` means any server can have access.) Any time you back up Cryptographic Security Platform Vault, it automatically stores the backup file in a folder called `/hcs/backup`. If you issue an NFS `mount` command to that directory from another server, you can access any of the backup files. Make sure these backup images are securely stored in case you ever need to restore Cryptographic Security Platform Vault. For details, see Network requirements and CSP Vault Backup and Restore.
Backup Over NFS	Whether backup over NFS is enabled. (Default: disabled.)
Cluster Operation Timeout	The amount of time that a Cryptographic Security Platform Vault node waits to receive a response from another Cryptographic Security Platform Vault node. If a response is not received by the specified timeout, the Cryptographic Security Platform Vault cluster goes into degraded mode, which indicates a network connectivity problem. Enter a value between 1 and 30 seconds. (Default: 5 seconds.) If a Cryptographic Security Platform Vault cluster frequently switches between degraded state and healthy state, you can increase this timeout. We recommend, however, that you keep the timeout as short as possible. Note: Typically, network latency is measured in milliseconds. Based on the clusters we have deployed at Amazon, the network latency from Northern California to Oregon was under ~100ms, North Virginia to Oregon was around ~200ms, and Northern California to Ireland was over ~280ms. The values varied based on time of day and the day of the week, but all values were considerably less than 5 seconds. If delays are consistently above 5 seconds, there is a network problem somewhere or a node is down.

Option	Description
Heartbeat Timeout	The number of seconds to wait for a Cryptographic Security Platform Vault heartbeat response between Cryptographic Security Platform Vault nodes in the cluster. If this time is exceeded, the heartbeat fails. Enter a value between 2 and 15 seconds. (Default: 3 seconds.)
Healthy Interval	The number of seconds between successful Cryptographic Security Platform Vault heartbeats for the cluster to be considered healthy. Enter a value between 1 and 10 seconds. (Default: 1 second.)
Degraded Interval	The number of seconds between failed Cryptographic Security Platform Vault heartbeats for the cluster to be considered degraded. Enter a value between 1 and 10 seconds. (Default: 1 second.)
Healthy Threshold	The number of successful consecutive heartbeats that must occur before Cryptographic Security Platform Vault determines that a degraded cluster is now healthy. Enter an integer between 2 and 10. (Default: 2.)
Degraded Threshold	The number of failed consecutive heartbeats that must occur before Cryptographic Security Platform Vault determines that a healthy cluster is now degraded. Enter a value between 2 and 10. (Default: 2.)

Any changes you make are communicated to all nodes in the cluster and take effect immediately.

Switching a Master Node

If you are using geographically distributed nodes in your cluster, and are having issues with performance, you can switch your master node to be the server closest to where the most data is being generated. When you switch your master node to a different node in the cluster, the cluster will automatically be placed in maintenance mode.

Note: This is especially beneficial for the Cryptographic Security Platform Vault for Cryptographic APIs and the Cryptographic Security Platform Vault for KMIP. Other vaults will not see a noticeable improvement.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab.
5. Select one of the nodes in the cluster.
   - The current mode is displayed in the Node column with a padlock next to the text Current Node.
   - The master node is displayed in the Server Name column with a star next to the name.
6. Select **Actions > Switch Master Node**.

7. Choose the server node that you want to make the new master and click **Continue**.
   This process can take several minutes.
   Note: If the process fails, you will see an error message with a retry button. After retrying, if it fails again, there may be an underlying issue with the server, and we recommend that you contact Support.
8. When the node switch has completed, click **Close** to close the window.
   The Cryptographic Security Platform Vault switches the master node and refreshes the **Servers** tab. At this point, the cluster is no longer in maintenance mode.

Choosing the Node Failover Order

The node failover order allows you to choose which node will become the master node after the master node is removed from the cluster. If you do not select a failover order, by default the next oldest node becomes the master. For example, if you have a disaster recovery node you do not wish to become the master, you can make it the last node in the failover order.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the System Settings section, click **Node Failover Order**.
5. Arrange the nodes in your preferred failover order, with the highest priority on top.
6. Click **Save**.

Startup Authentication

You can choose to enable passphrase-based startup authentication to provide further protection for the master key for all nodes in the same cluster. With passphrase-based startup authentication, the Cryptographic Security Platform Vault node will enter Recovery Mode every time it is rebooted. You will need to enter the passphrase in the Cryptographic Security Platform Vault webGUI. See the Recovery using Passphrase section in Recovering Access to CSP Vault

Startup Authentication allows Cryptographic Security Platform Vault to be used in tactical kits in hostile environments. Onsite staff can simply power off the Cryptographic Security Platform Vault nodes, which make them unusable until a passphrase or admin key is provided.

> Note: If Startup Authentication is enabled, you cannot add a new Cryptographic Security Platform Vault node. You must disable Startup Authentication first, add the new node, and then re-enable Startup Authentication.

- Enabling Startup Authentication
- Disabling Startup Authentication

Enabling Startup Authentication

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > Startup Authentication**.
6. In the Startup Authentication window, click **Edit**.
7. In the Passphrase Based Startup Authentication field, select **Enabled**.
8. Enter and confirm your passphrase.

The passphrase must be at least 12 characters long and include 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.

9. Click **Apply**.

Disabling Startup Authentication

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > Startup Authentication**.
6. In the Startup Authentication window, click **Edit**.
7. In the Passphrase Based Startup Authentication field, select **Disabled**.
8. Click **Apply**.

CSP Vault Backup and Restore

Cryptographic Security Platform Vault stores the configuration information, keys, and objects for all Cryptographic Security Platform Vault nodes in an encrypted object store that is shared among all nodes. Any changes you make on any Cryptographic Security Platform Vault node in the cluster is automatically disseminated to the other nodes in the cluster in a secure manner. This also allows you to backup all required information from any node in the cluster.

Important: Because encryption keys are stored in the Cryptographic Security Platform Vault backup file, you should create a new backup file every time you encrypt a new disk or rekey existing disks. If you restore Cryptographic Security Platform Vault from a backup file made before the disks were encrypted or rekeyed, the new keys will be lost and you will not be able to access the encrypted data.

You can back up Cryptographic Security Platform Vault using:

- The Cryptographic Security Platform Vault webGUI. The encrypted backup files Cryptographic Security Platform Vault creates can be downloaded locally or accessed through NFS on authorized servers. For details, see Backing Up CSP Vault Through the webGUI.
- A third-party application that can take and restore system snapshots. You can restore Cryptographic Security Platform Vault at any time from a previous snapshot, but if any part of the VM changes you may be required to recover the Admin key as described in Recovering Access to CSP Vault.

Note: If the cluster is degraded, you cannot perform a backup.

You can restore Cryptographic Security Platform Vault from a backup file using the Cryptographic Security Platform Vault webGUI. For details, see Restoring CSP Vault Through the webGUI.

Automatic Backup Feature

Cryptographic Security Platform Vault automatically creates a backup file once every 12 hours as long as the cluster is healthy. If this is the first time the automatic backup has completed successfully since the node was first initialized or restarted, Cryptographic Security Platform Vault records this information in the audit log. It does *not* send an alert or email to any Cryptographic Security Platform Vault users. It also does not record any subsequent successful backups.

The automatic backup schedule may change based on the following rules:

- If the cluster is in a degraded state, no automatic backup is attempted. The cluster must be healthy in order for Cryptographic Security Platform Vault to create a backup file.
- If the cluster is healthy but the automatic backup fails for some reason, Cryptographic Security Platform Vault retries the backup operation every hour. The first time the automatic backup fails Cryptographic

Security Platform Vault records this information in the audit log and alerts all Cryptographic Security Platform Vault accounts with Domain Admin privileges. It does *not* record subsequent failed backup attempts.
- Changes to the Cryptographic Security Platform Vault configuration may trigger an automatic backup, but it is better to backup Cryptographic Security Platform Vault manually whenever you make changes to be certain that you have an up-to-date backup file available.

Backing Up CSP Vault Through the webGUI

This procedure creates an encrypted backup file that can be downloaded through NFS on authorized servers or downloaded via the Cryptographic Security Platform Vault webGUI to the administrator's default download directory.

The backup file can later be used to restore Cryptographic Security Platform Vault to the state it was in when the backup was taken.

Before You Begin

If you have an enabled a Linux Access Control Policy on any of the VMs registered with Cryptographic Security Platform Vault, you must disable those Access Control Policies *before*you create the backup file. You can then re-enable the Access Control Policies after the backup is complete.

If you create the backup with any Linux Access Control Policies still active, you may be unable to access those VMs when you restore your Cryptographic Security Platform Vaultconfiguration from the backup file.

For details, see Removing Access Controls from a Disk.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. If you want to make the backup file available through NFS:
    a. Make sure the **Backup Over NFS** option is set to **Enabled**.
    b. Verify the IP addresses in the **Backup Hosts** field. If you want any server to have access to the backup directory, enter `0.0.0.0` .
6. Select **Actions > KeyControl Backup**. Cryptographic Security Platform Vault displays the latest backup information if one exists.
7. Click **Perform Backup**. Cryptographic Security Platform Vault creates a new backup file in the backup directory on the server and updates the information in this dialog box.
8. If you want to download the backup file locally, click **Download**. Cryptographic Security Platform Vault saves the encrypted backup file to your browser's default download location. The filename is in the format `<server-name>-<product_version><-datetimestamp>-<admin_key_version>.bu` .

If you want to access the backup file through NFS, log into one of the servers listed in the **Backup Hosts** field and mount the directory using the `mount` command. For example, if your Cryptographic Security Platform Vault node IP address is `192.168.140.135`, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

9. When you are done, click **Close**.

What to Do Next

If you disabled any Linux Access Control Policies for the backup, you can now re-enable those policies on the Linux VMs.

Backup and Restore Using the API

- Backup Image Status
- Create Object Store Backup Image
- Creating a Backup User
- Download Object Store Backup Image
- Restore Backup Image
- Restoring CSP Vault Through the webGUI
- Joining or Re-joining a Cryptographic Security Platform Vault Cluster
- Upload Backup Image

Backup Image Status

Returns information about backup image created using Create Object Store Backup Image.

Request

Method	URI
GET	v5/system_backup_status/

Privileges Required

DOMAIN_ADMIN or BACKUP_USER

Parameters

None.

Response

Name	Type	Example
backup_time	string	Thu Aug 3 21:19:21 2017
backup_exists	boolean	true

Name	Type	Example
backup_size	integer	1955390
backup_sha256	string	6286ea999404c730bfc6d9ba2629b216cd6debd8dd38cb4d1318de1025c66b76
result	string	success

Errors

Reason	Example
Unable to fetch backup information	Failed to retrieve backup details.

Create Object Store Backup Image

Creates a Cryptographic Security Platform Vault object store backup image on the Cryptographic Security Platform Vault node.

If you have an enabled a Linux Access Control Policy on any of the VMs registered with Cryptographic Security Platform Vault, you must disable those Access Control Policies *before*you create the backup file. You can then re-enable the Access Control Policies after the backup is complete.

If you create the backup with any Linux Access Control Policies still active, you may be unable to access those VMs when you restore your Cryptographic Security Platform Vaultconfiguration from the backup file.

Request

Method	URI
POST	v5/system_backup/

Privileges Required

DOMAIN_ADMIN or BACKUP_USER

Parameters

None.

Response

Name	Type	Example
result	string	success

Errors

Reason	Example
Backup image creation failed	Failed to create backup. No space available.

Creating a Backup User

Security Admin users can generate and download backup files. If you would prefer these actions to be performed by a more restricted account, for example if you are calling the APIs from a scheduled task, you can create a dedicated backup user. Backup users are users with the BACKUP_USER privilege, who can create, download, and view backups in both the webGUI and the API. Users who only have this role do not have any other admin access, and cannot access any other restricted APIs.

To create a user with the BACKUP_USER privilege, use a curl command similar to the following:

Copy

```
v=$(curl -s -k -d 'username=secroot&password=<password>' https://<IP-address>/v5/kc/login/ | jq .access_token| sed -e 's/"//g'); echo $v
curl -s -k https://<IP-address/v5/users/?access_token=$v -H 'Content-type: application/json' -d '{"email":"<backup@example.com>", "full_name":"<backup>", "login_name":"<backup@example.com>", "privileges": ["BACKUP_USER"], "account_enable":"Active"}' | tee qqq | jq .
```

Where:

- <password> is the password for the secroot user.
- <IP-address> is the IP address for your Cryptographic Security Platform Vault.
- <backup@example.com> is the email address to be used by the backup user.
- <backup> is the full name of the backup user.

Download Object Store Backup Image

Downloads the latest Cryptographic Security Platform Vault object store backup image available. The backup image can be created through the Cryptographic Security Platform Vault Management webGUI or the Create Object Store Backup Image method.

Request

Method	URI
GET	v5/system_backup/

Privileges Required

DOMAIN_ADMIN.

Parameters

None.

Response

Cryptographic Security Platform Vault backup file.

Errors

Reason	Example
Object store backup image not found	No backup available.

Restore Backup Image

This request restores Cryptographic Security Platform Vault using the backup file uploaded with the Cryptographic Security Platform Vault webGUI or the Upload Backup Imagemethod.

Warning: This is a destructive operation and should be used with care. If there has been is a hardware change since the backup file was created, you will be prompted to perform master key recovery after the restore operation has completed.

Request

Method	URI
POST	v5/restore_image/

Privileges Required

DOMAIN_ADMIN.

Parameters

None.

Response

Name	Type	Example
result	string	success

Errors

Reason	Example
Failed to restore object store image.	Multiple KeyControl nodes in the cluster. Excess KeyControl nodes must be removed before restore.

Restoring CSP Vault Through the webGUI

Restoring from a KeyControl backup should only be needed if there is a catastrophic failure in the Cryptographic Security Platform Vault cluster. If one Cryptographic Security Platform Vault node becomes unusable, for example due to hardware failures, simply remove the node from the cluster and add a new node.

Warning: Restore is a destructive process. Any changes made to objects created since the backup image was taken will be lost. This includes keys, policies, and Cryptographic Security Platform Vault user accounts. If the Cryptographic Security Platform Vault SSL certificate was changed since the backup was taken, the

older SSL certificate will be restored along with the rest of the system and the current SSL certificate will be discarded.

Custom SSL certificates for internal and external webservers will be restored only if the IP address specified in the certificate matches the Cryptographic Security Platform Vault IP address.

Note: If you are restoring a backup on Cryptographic Security Platform Vault with nShield HSM configured, you must do the following first:

- Initialize the Cryptographic Security Platform Vault node that you plan to restore to and copy its keyhash to the clipboard. You will need this keyhash to configure the HSM.
- Configure the nShield HSM to the new node before you start the restore process.
- Restore using a backup from the original Cryptographic Security Platform Vault.
- After the restore process, Cryptographic Security Platform Vault will go through admin key recovery.
- Select to recover the admin key using HSM.
- Provide the softcard name and softcard password used on the Cryptographic Security Platform Vault where the backup was created.
- After recovery, log in to the newly deployed Cryptographic Security Platform Vault and check that the admin key is available in the HSM.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Cluster**.
3. If there are any other nodes in this cluster, you must remove them before you restore the node. To do so:
    a. Click on the **Servers** tab.
    b. Click on each of the other nodes in the cluster and select **Actions > Remove**.
    c. Click **Proceed** at the prompt to confirm the request.
4. Go to the **Cluster** tab.
5. Select **Actions > Restore**.
6. Click **Browse** and select the backup file from which you want to restore Cryptographic Security Platform Vault. The name of the selected file appears next to the **Browse**button.
7. Click **Verify Image**. Cryptographic Security Platform Vault uploads the file and verifies that it is a valid backup file. It also displays a hint stating which Admin Key generation count goes with this backup file in case you need to upload the matching Admin Key parts. For example:
   Hint: Keypart generation version for this backup image is 16.
   For details, see Admin Keys.
8. Click **Restore Image**.
9. Click **Proceed** at the prompt to confirm the request. Cryptographic Security Platform Vault restores the system information from the backup file and reboots the server.
10. Verify the restoration by logging back into the Cryptographic Security Platform Vault Management webGUI. **Important:** Remember that all user account information has been reverted back to whatever it was when the backup was taken. That means your account may not exist or that the password may have changed.
11. If the hardware has changed since the backup was taken, Cryptographic Security Platform Vault presents you with additional options.

Option	Description
Recovery using Keypart upload	Allows you to recover the Admin key by uploading the parts from local files. You must upload the required number of parts of the Admin key within 10 minutes to use this method. Important: All Admin key parts must have the key generation count that was valid when the back up was taken. For details, see Admin Keys.
Recovery from External key server	Allows you to recover the Admin key by connecting to a server or HSM (Hardware Security Module).
Decommission	Tells Cryptographic Security Platform Vault to decommission the server. For more information, see Decommissioning a Cryptographic Security Platform Vault Node.

12. If you removed any nodes from the cluster, re-join them as described in Joining or Re-joining a Cryptographic Security Platform Vault Cluster.

Joining or Re-joining a Cryptographic Security Platform Vault Cluster

When you install Cryptographic Security Platform Vault, you can specify whether you want to configure the node as the first node in the system (standalone) or add it to an existing cluster.

If you ever need to change the node's cluster assignment, or you need to re-join a node with its previous cluster, you can do so using the Cryptographic Security Platform Vault webGUI installed on the node. You do not need to re-install the Cryptographic Security Platform Vault software.

Warning: When a node is added to a cluster, any existing configuration data and encryption keys are permanently deleted and cannot be restored. If this node was previously part of a different cluster or was used in standalone mode, make sure you do not need the encryption keys stored on this node before you add it to the new cluster.

Related Topics

Joining a Cryptographic Security Platform Vault Cluster

Re-Joining a Cryptographic Security Platform Vault Cluster

Joining a CSP Vault Cluster

The following procedure describes how to configure a newly deployed node to join an existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a CSP Vault Node from a Cluster.
- Make sure that you have tested the port connection between the joining node and the existing cluster node to ensure that they can communicate with each other. You can test the port connection through the console.

- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the same hostname for the Cryptographic Security Platform Vault node that it had originally. If you change the hostname, you will need to reinstall the externally signed SSL certificate on that node.
- A Cryptographic Security Platform Vault node cannot be joined to an existing Cryptographic Security Platform Vault cluster if the internal web server of the joining node is configured with a custom SSL certificate.
- Entrust recommends that you configure the Cryptographic Security Platform Vault node with a private IP address.

Procedure

1. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster.
2. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
3. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
4. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
5. Click **Continue**.
6. On the Download CSR page, click **Generate and Download CSR**.
7. Click **Continue**.
8. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
9. Select **Actions > Add a Node**.
10. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
11. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
12. Click **OK** to close the Add a Node window.
13. Return to the new node and click **Continue**.
14. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
15. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
16. When the node has successfully restarted, click **Login**.

What to Do Next

If necessary, update the list of Cryptographic Security Platform Vault IP addresses on the VMs associated with this cluster. If you are maintaining the list of IP addresses on the VMs, see Updating Cryptographic Security Platform Vault Node IP Addresses on an Individual VM. If you are using Cluster Node Mappings, see Changing a Cluster Node Mapping.

If you are using an HSM, see the appropriate link to rejoin the cluster:

- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration

Re-Joining a CSP Vault Cluster

The following procedure describes how to configure a node that has been in use as either a standalone node or part of a cluster to join another existing Cryptographic Security Platform Vault cluster.

Important: This process will destroy all data on the node.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a CSP Vault Node from a Cluster.
- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the same hostname for the Cryptographic Security Platform Vault node that it had originally. If you change the hostname, you will need to reinstall the externally signed SSL certificate on that node.

Procedure

1. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Select **Actions > Join a Cluster**.
   The Join Existing Cluster window displays.
5. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. The passphrase must contain 12 alphanumeric characters. It *cannot* contain spaces or special characters. This phrase is a temporary string used to encrypt the initial communication between this node and the existing Cryptographic Security Platform Vault cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
6. Confirm that you understand that all existing data on this node will be deleted by typing "delete my data".
7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.

13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address or hostname of any node in the existing cluster, and enter the passphrase that you selected.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.

What to Do Next

If necessary, update the list of Cryptographic Security Platform Vault IP addresses on the VMs associated with this cluster. If you are maintaining the list of IP addresses on the VMs, see Updating Cryptographic Security Platform Vault Node IP Addresses on an Individual VM. If you are using Cluster Node Mappings, see Changing a Cluster Node Mapping.

If you are using an HSM, see the appropriate link to rejoin the cluster:

- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration

Upload Backup Image

This is the first step of restoring Cryptographic Security Platform Vault. This request uploads and verifies the Cryptographic Security Platform Vault backup file that you want to use.

Request

Method	URI
POST	v5/verify_image/

Privileges Required

DOMAIN_ADMIN.

Parameters

Name	Type	Example
file	Object store backup image	KC2.localdomain-201708032119.bu

Response

Name	Type	Example
result	string	success

Name	Type	Example
keypart_generation	string	6

Errors

Reason	Example
Failed to verify backup image.	Image verification failed.

Removing a CSP Vault Node from a Cluster

You can remove and later re-join nodes that are unreachable for an extended time due to maintenance or other issues. Because there may be multiple administrators for this appliance, please ensure that all other administrators are aware of any changes that you make to the cluster.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node you are *not* removing using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab.
5. Select the node or nodes that you want to remove.
   Important: All unreachable nodes need to be removed together. To remove multiple nodes, click the **Multi-Select** checkbox at the top-right of the page.
6. Select **Actions > Remove**.
7. Click **Proceed** at the prompt to confirm the request.
8. Cryptographic Security Platform Vault removes the node and refreshes the **Servers** tab.

What to Do Next

If you want to rejoin the node to an existing Cryptographic Security Platform Vault cluster, see Joining or Re-joining a CSP Vault Cluster.

If you want to remove the node permanently, see Decommissioning a CSP Vault Node.

Changing the IP Address for a Node

After you have deployed a Cryptographic Security Platform Vault node, you cannot change its IP address, hostname, or domain name. In order to work around this restriction, you can do the following:

1. Deploy a new Cryptographic Security Platform Vault node using the IP address and hostname you want to use and join it with the original node to form a cluster.
   For details, see Installation Overview.
2. Update any Cluster Node Mappings that you have defined in your environment to use the new node. If you are replacing a standalone node, you must then make sure the new Node Mapping information has been successfully disseminated to all registered VMs before you continue. For more information, see High Availability Between a VM and the CSP Vault Cluster.
3. If there are any VMs that are registered directly with the old Cryptographic Security Platform Vault node, you need to update the Cryptographic Security Platform Vault list on those VMs or create a Cluster Node Mapping and assign that Node Mapping to the VMs. For details see Updating CSP Vault Node IP Addresses on an Individual VM or Managing the Cluster Node Mapping on a VM.

Tip: We highly recommend that you use a Cluster Node Mapping instead of registering VMs directly with Cryptographic Security Platform Vault to provide more flexibility and high availability between the VM and Cryptographic Security Platform Vault.

4. When all VMs have been updated to use the new Cryptographic Security Platform Vault IP address, you can decommission the old Cryptographic Security Platform Vault node as described in Decommissioning a CSP Vault Node or you can simply remove it from the cluster and destroy the VM as described in Removing a CSP Vault Node from a Cluster.

Rebooting a CSP Vault Node

You can only reboot the node that you are currently using.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Servers** tab.
5. Select **Actions > System Reboot**.
6. Click **Proceed** to acknowledge the warning message.

Decommissioning a CSP Vault Node

Before You Begin

- Make sure the node is not part of a cluster before you decommision it. For details, see Removing a CSP Vault Node from a Cluster.
- Make sure you have access to all of the key parts for the Admin key that was generated for this system. All of the parts need to be uploaded within 10 minutes of the first file upload in order for the decommission to work.
  If there are multiple system administrators, each administrator has one of the key parts. You can either collect the parts and have one administrator upload them all or you can have each administrator log in and upload their part simultaneously.
  For this procedure you *must* use the Admin Key parts that were sent to the Security Administrators. You cannot use the Admin Key stored on an external key server.

Warning: When you decommission a Cryptographic Security Platform Vault node, Cryptographic Security Platform Vault uses zeroization to completely erase the data on the disks where the Cryptographic Security Platform Vault software and the object store are located. This is a non-reversible procedure.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI on the node you want to decommision using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **System Decommission**.
5. Click **Browse** to upload the first part of the admin key. Navigate to the key part and click **Choose**. The filename of the key part replaces the text of the **Browse** button.
6. Click **Upload File**.
7. If there is only one admin key part, Cryptographic Security Platform Vault immediately logs you out of the system and zeroes out the disks associated with the Cryptographic Security Platform Vault node. If there are multiple key parts, Cryptographic Security Platform Vault starts a 10 minute timer. All admin key parts must be uploaded within the 10 minutes before Cryptographic Security Platform Vault will decommission the node.

8. If you need to restart the process, click **Reset**. You will need to re-upload all key parts to complete the process.

Enabling or Disabling the Support Login

You must enable support accounts before support personnel from Entrust can access your system. When the account is enabled, support personnel have full access to the system to carry out diagnosis and repairs in exceptional situations.

You can disable the support account after using, for example, after a successful upgrade, or else the support login will automatically be disabled after 24 hours.

1. Log into the Cryptographic Security Platform Vault webGUI using an account with Security Administrator or Cloud Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the node or nodes that you want to modify.
5. Select **Actions** and under the Support Login Settings section, select **- Full Access**.
   Note: If restricted access is all that is required, you can select **- Restricted Access** instead.
6. On the Full Support Login Settings page, check the Enable Full Support Login checkbox.
7. Enter and confirm the password for the support login.
   The password must be at least 8 characters long, including 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.
8. Click **Save**.
9. If the support login is enabled, you can disable it by checking the Disable Full Support Login checkbox and clicking **Save**.

Accessing CSP Vault Backup Files

If you want to access an existing Cryptographic Security Platform Vault backup file, you can use the Cryptographic Security Platform Vault Management webGUI, the Entrust Cryptographic Security Platform Vault API or, if you have configured an NFS server, you can use NFS.

The following sections describe how to access the backup file through the webGUI and NFS.

Cryptographic Security Platform Vault Management webGUI Access

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > KeyControl Backup**. Cryptographic Security Platform Vault displays the latest backup information if one exists.
6. Click **Download**. Cryptographic Security Platform Vault saves the encrypted backup file to your browser's default download location. The filename is in the format `<server-name>-<product_version>-<datetimestamp>-<admin_key_version>.bu`.
7. Click **Close**.

NFS Access

To access the backup file through NFS, log into one of the Backup Host servers configured for the cluster and mount the directory using the `mount` command. For example, if your Cryptographic Security Platform Vault node IP address is `192.168.140.135`, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

CSP Vault System Maintenance and Troubleshooting

CSP Vault Activity Tracking

Cryptographic Security Platform Vault tracks all activity on the system in the audit log. Users can export the audit log from the webGUI but they cannot change it in any way. For security reasons, Cryptographic Security Platform Vault tracks most of the events in the system.

For important events, Cryptographic Security Platform Vault makes an entry in the audit log and also raises an alert. Users can look at the Alert tab in the webGUI to get a quick overview of the major events that have taken place in the system. webGUI users can delete an alert from their local view, but the same alert will still be visible to other Cryptographic Security Platform Vault users who have the same Cryptographic Security Platform Vault permissions.

Cryptographic Security Platform Vault categorizes audit log messages and alerts based on both the user's administrative roles (Cloud Admin, Domain Admin, and Security Admin) and the groups to which the user belongs. When a user logs into the webGUI, they can see the audit log messages and alerts generated by their groups that correspond to the privileges associated with their account. For example:

- If a Security Administrator logs in, they will see an alert if a user account is locked because a user exceeded the maximum number of consecutive failed login attempts. Security Administrators are not assigned to a group, so all Security Administrators see all security alerts.
- If a Cloud Administrator logs in, they will see an alert if a new Cloud VM Set has been created in one of the Cloud VM Sets in their associated groups. They will not see an alert about Cloud VM Sets created in other groups.
- If a Domain Administrator logs in, they will see an alert if a new Cryptographic Security Platform Vault node has been added to the cluster.
- If someone with Security, Cloud, and Domain Admin privileges logs in, they will see all three of the alerts mentioned above.

In addition to viewing alerts in the webGUI, administrators can also receive alerts by email depending on how the system is configured. For details, see Setting Email Server Preferences.

For a list of audit log messages, see CSP Vault Audit Messages.

- Managing Alerts
- Viewing the Audit Log
- Configuring Audit Log Settings

- Exporting the Audit Log

Managing Alerts

Cryptographic Security Platform Vault categorizes alerts based on both the user's administrative roles (Cloud Admin, Domain Admin, and Security Admin) and the groups to which the user belongs. When a user logs into the webGUI, they can see the alerts generated by their groups that correspond to the privileges associated with their account. For details, see CSP Vault Activity Tracking.

> Note: Cryptographic Security Platform Vault keeps a maximum of 500 alerts per user. If this amount is exceeded, Cryptographic Security Platform Vault deletes the oldest alert when a new alert is generated.

Viewing Alerts

In the top menu bar, click Alerts.

Copying and Filtering Alerts

To copy an alert to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple alerts, click the Multi-Select button and then left-click on the alerts you want to select.

To filter the alert list:

1. In the **Filter** drop-down list, select the field that you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search tips for the available field types:

- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the alert was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.

Deleting Alerts

To delete one or more alerts from your local view:

1. Select the alerts you want to delete.
2. Select **Actions > Delete Alerts**.

If you need to see an alert you previously deleted, you can find it in the Audit Log. For details, see Viewing the Audit Log.

Viewing the Audit Log

CSP Vault generates detailed records that document activities and events associated with the Key Management System. Among these records, audit logs capture auditable events and can be accessed through multiple interfaces of Cryptographic Security Platform Vault, including the REST API, CLI, or the GUI. These logs serve as a comprehensive, chronological archive, facilitating the tracking of changes, access, and various operations. They are frequently utilized for understanding system behavior, diagnosing issues, and conducting security audits.

Audit logs offer flexibility in how they are consumed, and they can be exported in user-friendly CSV or XML formats or forwarded to an external syslog server for centralized logging and analysis.

The following table describes the audit log parameters:

Parameters	Description
Time	Date and time when the event was created.
Type	The severity of the record. The severity types are: • INFORMATION • CRITICAL • WARNING • ERROR
User	The user who initiated the operation.
Message	The operation and details associated with the operation performed.

How you access the audit log in the webGUI depends on which vault you using.

- For the Cryptographic Security Platform Vault Management webGUI, the Cryptographic Security Platform Vault for Cloud Keys webGUI, the Cryptographic Security Platform Vault for Databases webGUI, or the Cryptographic Security Platform Vault for VM Encryption webGUI, click **Audit Log** in the top menu bar.
- For the Cryptographic Security Platform Vault for Cryptographic APIs webGUI, the Cryptographic Security Platform Vault for KMIP webGUI, or the Cryptographic Security Platform Vault for Secrets webGUI, click **Audit Log** on the main page.

To view the details for a given message, click the Expand button > at the end of the row.

To copy a message to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple rows, click the Multi-Select button and then left-click on the rows you want to select. If you want to export the entire audit log in CSV or XML format, see Exporting the Audit Log.

You can filter the audit log messages displayed using one or more text searches forming an AND search string. The webGUI displays the selected filters below the field. To remove a particular filter, click the X following the filter name.

All searches are partial word and case-insensitive. So "cre" would match "Create" and "Secret".

You cannot use regular expressions and you cannot specify a NOT condition in the search string. Complex searches can only be done through the API.

To filter the message list:

1. In the **Filter** drop-down list, select the field you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search Tips by Field Type

- Category—Common categories are Security and Clusters.
- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the log entry was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.
- Group—The name of the associated group, such as KeyControl Admin Group and Cloud Admin Group.
- Host—The hostname of the server where the activity took place. In general this will be one of the Cryptographic Security Platform Vault nodes.

- ID—The message ID. For example, if you want to see all messages where a Cloud VM Set was created, you would enter "12" in the filter field.
- User—Searches the text shown in the **User** column. For a user-defined webGUI account, this will be the Full Name specified for the account. For security reasons, the user login ID is not saved in the Audit Log.

Configuring Audit Log Settings

You can choose to retain audit logs depending on size, retention period, or both.

- The audit log retention policy (by size or retention period) is enforced every 10 minutes starting from system startup.
- Audit log retention by size is approximate:
  - If an audit is added to the log while the system is in this enforcement period, the size of the audit log may increase temporarily.
  - If an audit is in process when the enforced size is reached, then that audit is retained in the log and the rest are deleted.

If you want to use an external syslog server, see Configuring Syslog Server Settings.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Audit Log** and specify the options you want to use. The Cryptographic Security Platform Vault Management webGUI automatically saves your changes as you make them.

Option	Description
Log Retention	The Cryptographic Security Platform Vault webGUI displays the number of days for which it will keep old audit log messages. The default is 90 days. Click this value to set a new retention time. The minimum retention time allowed is 30 days. If you check the Retain All checkbox, then Cryptographic Security Platform Vault will never delete old messages from the audit log.
Maximum Log Size	The default is Unlimited, which means Cryptographic Security Platform Vault never deletes old messages from the audit log based on the size of log. To change this value, click Unlimited then enter an integer and select MB, GB, or TB in the units list box. The log size must be *at least* 10 MB. If you have changed the size and want to restore the default Unlimited setting, specify 0 (zero) in this field.

Exporting the Audit Log

You can export the audit log in CSV (comma-separated value) or XML format. Cryptographic Security Platform Vault stores the audit log until you can download it.

CSV Format

To download the entire audit log or selected audit log rows in CSV (comma-separated value) format:

1. If you want to download a subset of audit log messages, select the appropriate rows. If you have filtered the list, you can export just the filtered items without selecting them first.
2. Select **Actions > Export**.
3. Select **CSV** in the **Format Type** drop-down list.
4. In the **Which Rows?** drop-down list, select:
   All Loaded—Downloads the audit log messages that match the selected filters, if any. If there are no filters, this option downloads all audit log messages.
   Selected—Downloads just those audit log messages selected in the webGUI using the **Multi-Select** option.
5. In the **Which Columns?** drop-down list, select **All**.
6. Click **Generate**.
   Cryptographic Security Platform Vault generates a file called `htdc-auditlog-datetimestamp.csv`.
   The `datetimestamp` is in the format month, day, year, hour, minute, seconds, AM/PM. For example, `htdc-auditlog-4-6-2017--11_41_49-AM.csv`.
7. After the audit log has finished generating, click **Download**.

XML Format

1. Select **Actions > Export**.
2. Select **XML** in the **Format Type** drop-down list.
3. Click **Generate**.
   Cryptographic Security Platform Vault generates a file called `htdc-auditlog-datetimestamp.xml`.
   The `datetimestamp` is in the format month, day, year, hour, minute, seconds, AM/PM. For example, `htdc-auditlog-4-6-2017--11_41_49-AM.xml`.
4. After the audit log has finished generating, click **Download**.

Moving a CSP Vault Node to a New Server in a Multi-Node Environment

If you want to move a CSP Vault node to a different server, you can simply remove the old server and then install the Cryptographic Security Platform Vault software on the new server and join the new server to the cluster so that the object store is copied to the new server and all your configuration settings are retained. As long as one node remains in the cluster, you can change the other servers out as needed.

> Note: If you want to move a Cryptographic Security Platform Vault node in a single-node system, see Moving a CSP Vault Node to a New Server in a Single Node Environment.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node you are *not* moving using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the Cryptographic Security Platform Vault node that you want to move and select **Actions > Remove**.
5. Log into the existing server as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
6. Select **Shutdown System** from the Entrust Cryptographic Security Platform Vault System Console.
7. Optionally, uninstall Cryptographic Security Platform Vault as described in Decommissioning a CSP Vault Node.
8. Decommission or re-purpose the server as needed.
9. Set up the new hardware and install Cryptographic Security Platform Vault as an additional node in an existing cluster. For details, see CSP Vault ISO Installation for Hypervisors or CSP Vault OVA Installation. If possible, make sure the new system uses the same IP address as the old system so that all Policy Agents can find the new systems. If you need to change the system IP address, you need to update the

appropriate Cluster Node Mappings or update the list of authorized IP addresses with each Policy Agent as described in Changing a Cluster Node Mapping and Updating CSP Vault Node IP Addresses on an Individual VM.

Moving a CSP Vault Node to a New Server in a Single Node Environment

If you want to move a Cryptographic Security Platform Vault node to a different server, you can install the Cryptographic Security Platform Vault software on the new server and join the new server to the cluster so that the object store is copied to the new server and all your configuration settings are retained. Then you can remove the old server from the cluster and decommission it.

> Note: If you want to move a Cryptographic Security Platform Vault node in a multi-node cluster, see Moving a CSP Vault Node to a New Server in a Multi-Node Environment.

Procedure

1. Set up the new server and install Cryptographic Security Platform Vault as an additional node in a cluster with the old Cryptographic Security Platform Vault node. For details, see CSP Vault ISO Installation for Hypervisors or CSP Vault OVA Installation.
   Make note of the IP address you assigned to the new server.
2. Make sure your new node is properly configured by logging into the Cryptographic Security Platform Vault Management webGUI on the new server using an account with Domain Admin privileges.
   Note: If you are using Cluster Node Mappings, you need to log in using an account with Cloud Admin privileges as well in order to update the Mappings later in this procedure.
3. In the top menu bar, click **Cluster**. The cluster **Status** should be **Healthy** and both nodes should appear on the **Servers** tab.
4. If you have registered the Cryptographic Security Platform Vault IP address directly on each Policy Agent (as opposed to using a Cluster Node Mapping), log into each server connected to Cryptographic Security Platform Vault and issue the command:
   ```
   # hcl updatekc kc_hostname[:port]
   ```
   Where `kc_hostname` is the IP address of the new server and `port` is an optional port number if the port is anything other than the default (443).
5. If you set up one or more Cluster Node Mappings, you need to update them:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI.
   b. In the top menu bar, click **Workloads**.
   c. Click the **Mappings** tab.
   d. Select the Node Mapping in the list, then select **Actions > Edit Mapping**.
   e. Add the new Cryptographic Security Platform Vault node to the Node Mapping and then remove the old Cryptographic Security Platform Vault node.
   f. Click **Update**.
   g. The new Cluster Node Mapping will be communicated to the associated Policy Agents on the next heartbeat. You can either wait for that to happen to make sure the agents are using the new Cryptographic Security Platform Vault IP address or you can log into the VMs and run the command `hcl updatekc –a`.
6. After all VMs in the system are using the new Cryptographic Security Platform Vault IP address, you can remove the old node and decommission the server.
   Important: If you are using Cluster Node Mappings, make sure that the Node Mapping information has updated on all the VMs registered with Cryptographic Security Platform Vault before you remove the old node from the cluster. Just changing the Node Mapping in Cryptographic Security Platform Vault is not enough. Each VM *must* heartbeat with Cryptographic Security Platform Vault *before* the change in the Node Mapping file can be disseminated to the VM. If you remove the old node before this happens, the VM will be unable to connect to Cryptographic Security Platform Vault and access to the encrypted data on the VM could be lost.

a. Log into the Cryptographic Security Platform Vault Management webGUI.
b. In the top menu bar, click **Cluster**.
c. Click the **Servers** tab.
d. Click the old node in the list and select **Actions > Remove**.
e. Log into the existing server as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
f. Shut down the server by selecting **Shutdown System** from the Entrust Cryptographic Security Platform Vault System Console.
g. If desired, uninstall Cryptographic Security Platform Vault as described in Decommissioning a Cryptographic Security Platform Vault Node.
h. Decommission or re-purpose the old server as needed.

Increasing CSP Vault Storage in a VM

If you installed Cryptographic Security Platform Vault in a VM, you can increase the amount of storage available without reinstalling Cryptographic Security Platform Vault. You just need to increase the size of the underlying disk and reboot the Cryptographic Security Platform Vault node.

Important: If you upgraded to Version 10.5.3, you must delete the pre-upgrade snapshots before you start. See Delete CSP Vault Snapshots.

1. Increase the size of the virtual disk in which Cryptographic Security Platform Vault is installed using your hypervisor tools.
   Note: You may need to shut down the VM before you can resize the disk. For details, see your hypervisor documentation.
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Cluster**.
5. Select the Cryptographic Security Platform Vault node whose disk you just resized in the list.
6. Select **Actions > System Reboot**.
7. If necessary, log back into the webGUI after the Cryptographic Security Platform Vault node has rebooted.
8. Review the Audit Log messages. The node should report the new size upon success or provide information if the resize failed.

VM Handlers for Attach/Detach in Linux

There are scripts that are invoked when a device is either attached or detached. These scripts can be found under the `/opt/hcs/handlers` directory. The attach handler (`default.attach`) is invoked when a new device is attached and the detach handler (`default.detach`) is invoked when a new device is detached.

The default attach handler is shown below:

```
#!/bin/sh

# Post-attach handlers are called with at least 2 and at most 4 arguments:
# 1. the absolute path of the cleartext device e.g. /dev/mapper/clear_sda
# 2. the absolute path of the encrypted_device e.g. /dev/sda
# 3. (optional) mountpoint
# 4. (optional) mount options
# If the mountpoint and mount options are supplied, then the default handler
# will fsck and mount the cleartext device on the given mount point.
```

```
if [ $# -lt 2 -o $# -gt 4 ]; then
   exit 1
fi
if [ $# -eq 2 ]; then
   exit 0
fi

cleardev=$1
if [ $# -ge 3 ]; then
   mntpt=$3
fi
if [ $# -eq 4 ]; then
   mntopts=$4
fi

fsck -a "$cleardev"
if [ $? -eq 0 ]; then
   mount $mntopts "$cleardev" "$mntpt"
else
   exit 2
fi
```

The mount point and mount options are collected along with the clear-text path to the device and a mount call is made.

The handlers can be changed freely. We recommend that you back up your handlers, using your preferred backup solution.

VM Handlers for Attach/Detach in Windows

The windows client also supports attach and detach handler scripts, located at `c:\Program Files\hcs\handlers`. These run at the same times as the Linux client scripts. The attach handlers will be called immediately after a successful attach. Detach handling scripts will be called immediately before detaching disks.

You can create a handler script for each disk that is encrypted. The format of the name will be:

`DRIVE_LETTER.attach.cmd` and `DRIVE_LETTER.detach.cmd`

Individual disk handler scripts are not required. If not specified, then the default script will be called instead. Those are named `default.attach.cmd` and `default.detach.cmd`.

Each script invocation will be passed the following parameters:

1. The drive letter of the disk being attached or detached. This parameter will be an empty string if the encrypted partition does not have a drive letter assigned.
2. The device name of the volume that is being attached or detached.
3. The index into the list of encrypted drives. The index values start at 0. For example, if there are 4 encrypted drives, the index values will go from 0 to 3 as each drive is attached or detached.
4. The total number of encrypted drives. If this value is 0, it indicates that only a single disk has been attached or detached from the command line (for example, by an administrator issuing the `hcl attach` or `hcl detach` command or by revoking or restoring a disk with the Cryptographic Security Platform Vault webGUI).

The script can determine if all disks are attached or detached by comparing parameters 3 and 4. If parameter 3 (plus 1 because it is offset from 0) is equal to parameter 4, then the script can assume that all of the disks

in the system have been handled. If the total number of disks passed in is 0, that indicates that only a single disk is being operated on at that time.

If you have a disk that already contains data that you want to be encrypted, you can run the `hcl encrypt` command. All encryption, whether encrypting a new disk or removing and decrypting an existing disk, makes use of dynamic rekey. In the case of encrypting a disk, we do the conversion in the background, thus allowing you access the disk while the encryption process is taking place. This allows you to have no downtime for your applications and data.

> Note: If Windows disks are sparse, we will only encrypt allocated blocks ensuring that only the allocated blocks are encrypted and the sparseness remains. This is not currently available for Windows `C:` drives.

To demonstrate how rekey works, let's first look at the contents of the unencrypted `G:` :

```
C:\>dir g:

 Volume in drive G is New Volume
 Volume Serial Number is 44A1-E6A7

 Directory of G:\

10/25/2022  01:48 PM           346,454 HCS_BreachWhitepaper_v1.5.pdf
10/25/2022  01:48 PM           303,179 HCS_CSP_Whitepaper.pdf
10/25/2022  01:48 PM         2,278,559 HCS_Encryption_Use_Cases.pdf
10/25/2022  01:48 PM           883,773 HCS_HIPAA_Compliance.pdf
10/25/2022  01:48 PM         1,006,858 HCS_PCI_Compliance.pdf
10/25/2022  01:48 PM           310,103 HCS_Shack-P1.pdf
10/25/2022  01:48 PM           495,492 HCS_Shack-P2.pdf
               7 File(s)      5,624,418 bytes
               0 Dir(s)   2,098,798,592 bytes free
```

Now let's start the encryption process:

```
C:\>hcl encrypt g:
All the data on G: will be encrypted. This operation may take a long time.
Do you want to proceed? (y/n) y

registering drive G:, guid FF2A17F2-D7DE-404B-B977-018ADC611BCC

Encrypted device G: has been added.
```

You can view the progress of the rekey operation by running `hcl rekey` as follows:

```
C:>\hcl rekey status g:

device: \Device\Harddisk3\Partition1
drive: G
state: in progress
begin: 65536
end: 2144403456
current: 725794816
sector offset (from 0): 1417568
total sectors: 4188160
total size: 2144337920
```

pct done: 33.85%
elapsed time (seconds): 27

Even though the drive is only partially encrypted, we can still view the contents:

C:\>dir g:

Volume in drive G is New Volume
Serial Number is 44A1-E6A7

Directory of G:\

10/25/2022 01:48 PM 346,454 HCS_BreachWhitepaper_v1.5.pdf
10/25/2022 01:48 PM 303,179 HCS_CSP_Whitepaper.pdf
10/25/2022 01:48 PM 2,278,559 HCS_Encryption_Use_Cases.pdf
10/25/2022 01:48 PM 883,773 HCS_HIPAA_Compliance.pdf
10/25/2022 01:48 PM 1,006,858 HCS_PCI_Compliance.pdf
10/25/2022 01:48 PM 310,103 HCS_Shack-P1.pdf
10/25/2022 01:48 PM 495,492 HCS_Shack-P2.pdf
7 File(s) 5,624,418 bytes
0 Dir(s) 2,098,798,592 bytes free

Upgrading to a New Hardware Signature Format

To ensure security, Cryptographic Security Platform Vault periodically upgrades the hardware signature format. When you upgrade your Policy Agent, you may see an alert message similar to "VM is using an older Hardware Signature format. Please run “hcl auth” cmd on the VM for a more secure signature".

This means that the hardware signature format on the policy agent has been updated. In order to use the new hardware signature format, you will need to reauthorize your client by running the `hcl auth -a` command inside Windows or Linux after the system is fully booted.

> Note: If you run the `hcl auth` command without the `-a` option, the encrypted disks will be detached during the reauthorization process.

Important: Although upgrading the hardware signature is optional, we highly recommend that you run the command when you see this alert.

Troubleshooting Network Issues

To ensure security, Cryptographic Security Platform Vault periodically upgrades the hardware signature format. When you upgrade your Policy Agent, you may see an alert message similar to "VM is using an older Hardware Signature format. Please run “hcl auth” cmd on the VM for a more secure signature".

This means that the hardware signature format on the policy agent has been updated. In order to use the new hardware signature format, you will need to reauthorize your client by running the `hcl auth -a` command inside Windows or Linux after the system is fully booted.

> Note: If you run the `hcl auth` command without the `-a` option, the encrypted disks will be detached during the reauthorization process.

Important: Although upgrading the hardware signature is optional, we highly recommend that you run the command when you see this alert.

Cleaning Up Stale Tasks

In some rare scenarios, CSP Vault fails to track some tasks. The state of those tasks is 'In Progress' and it is never updated. Because Cryptographic Security Platform Vault automatically sends delayed task alerts for inactive tasks every 6 hours, you will continue to receive alerts from those stale tasks until they are marked abandoned.

You can abandon tasks for VMs or Cloud VM Sets. The abandoned tasks will be cleared in 24 hours.

Important: Do not use this option to stop a task.

Marking Tasks as Abandoned Using the webGUI

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Cloud Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Workloads**.
4. Navigate to either the **VM Sets** or **VMs** tab.
5. Select the Cloud VM Set or VM that has inactive tasks.
6. Select **Actions > Abandon Inactive Tasks**.
7. In the confirmation window, click **Proceed**.

Marking Tasks as Abandoned Using the hicli

Log in to the hicli and select one of the following options:

- Abandon a task by the task ID:
  ```
  hicli cvmset abandon_task <cvmset_name> --taskid=<taskid>
  ```
- Abandon all tasks that have been inactive for 6 days or more on a Cloud VM Set:
  ```
  hicli cvmset abandon_inactive_tasks <cvmset_name>
  ```
- Abandon all tasks that have been inactive for 6 days or more on a VM:
  ```
  hicli cvm abandon_inactive_tasks <cvm_name>
  ```

Support Access and Log Files

Entrust Cryptographic Security Platform Vault provides two methods of support access:

- Restricted support—Customers can access support logs and run simple diagnostic tools through a limited SSH-accessible shell that can be invoked from the Entrust Cryptographic Security Platform Vault System Console. For details, see Using the Restricted Shell.
- Full support—The Entrust support staff can access and troubleshoot the customer's system. Full support access requires multi-factor authentication between the Cryptographic Security Platform Vault Administrator at the customer site and Entrust Support. If such access is required, Entrust Support will guide you through the process.

- Recovering Access to CSP Vault

Using the Restricted Shell

The restricted support login provides a limited SFTP-accessible shell in which the Cryptographic Security Platform Vault administrator can gather diagnostic information. It is disabled by default.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts** and press **Enter**.
3. On the Manage Accounts page, select **htrestricted (read only support access)** and press **Enter**.
   The TUI displays the Manage the htrestricted account page.
   Note: If the account is currently enabled, Cryptographic Security Platform Vault displays that information along with the date on which the current restricted support password will expire. If you want to set a new password, select **Yes** at this prompt and then return to step 2.
4. Select **Yes** and press **Enter** to confirm the request.
5. Enter the password for the `htrestricted` support account. When you are done, select **OK** and press **Enter**, then press **Enter** again to confirm the request.
6. Use SFTP to log into the `htrestricted` account on the Cryptographic Security Platform Vault node using the password you specified above.
   Tip: Windows users can use WinSCP to access the `htrestricted` account via SFTP.
   The following example shows how to log into the restricted shell and navigate to the directory containing the latest support bundles. The first bundle contains the logs for the current node only, while the second bundle contains the logs from all nodes in the cluster:

```
$ sftp htrestricted@10.238.66.250
htrestricted@54.193.4.110's password:
Connected to htrestricted@54.193.4.110.
sftp> cd support/logs/node_logs
sftp> ls
htkc_dbginfo_kc-250.domain.mycompany.com_2019-07-03-21-27-57.tar.gz
sftp> cd ../cluster_logs
sftp> ls
htkc_cluster_dbginfo_2019-07-03-21-29-11.tar.gz
sftp>
```

   For details about using the restricted shell, contact Entrust Support.

Creating a Support Bundle with the webGUI

In certain circumstances it may be necessary to gather diagnostic information and logs from Cryptographic Security Platform Vault that can be sent to Entrust support for further analysis. The following procedure describes how to create a log bundle using the webGUI. To create the bundle with the Entrust Cryptographic Security Platform Vault System Console on the Cryptographic Security Platform Vault node, see Creating a Support Bundle from the Entrust CSP Vault System Console.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Support** section, click **Download Logs**.
5. If a log has not yet been created for this cluster or if you want to generate a new log, click **Create Bundle**.

6. In the Logs dialog box, enter the following information:

Option	Description
Include Audit Log	If Yes, Cryptographic Security Platform Vault includes the full audit log in the bundle. The default is Yes.
Include All Cluster Logs	If Yes, Cryptographic Security Platform Vault includes the log bundle from every Cryptographic Security Platform Vault node in the cluster. If No, Cryptographic Security Platform Vault only includes the log bundle from the current node. The default is No.
Include Core Files	If Yes, Cryptographic Security Platform Vault includes core files in the bundle. The default is No.
Passphrase	If you specify a passphrase, Cryptographic Security Platform Vault encrypts the bundle with an AES 256-bit key using the provided passphrase.

7. When you are done, click **Create**. Cryptographic Security Platform Vault creates the log file and then refreshes the information about the log bundle it created.
8. To download the bundle, click **Download**.
   Tip: Some browsers may display a warning that the log bundle is not commonly downloaded and may be dangerous. It is safe to ignore this message and continue the download.

Note: If you want to decrypt the log bundle, navigate to the directory where the bundle is located and type the following command:

gpg -d -o <output-file-name> <input-file-name>

Where `<output-file-name>` is the name you want to use for the decrypted log bundle and `<input-file-name>` is the name of the encrypted log bundle that you want to decrypt.

Creating a Support Bundle from the CSP Vault System Console

In certain circumstances it may be necessary to gather diagnostic information and logs from Cryptographic Security Platform Vault that can be sent to Entrust support for further analysis. The following procedure describes how to create a log bundle using the Entrust Cryptographic Security Platform Vault System Console on one of the nodes in the cluster. To create the bundle using the webGUI, see Creating a Support Bundle with the webGUI.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Gather Diagnostic Logs**.
3. In the Create Log Options page, use the arrow keys to move to an option you want to change and then use the spacebar to toggle whether that option is selected. When you are done, press **Enter**. The options are:

Option	Description
Include Audit Log?	If selected, Cryptographic Security Platform Vault includes the full audit log in the bundle. This option is selected by default.
Include Log Bundle from ALL KeyControl Nodes?	If selected, Cryptographic Security Platform Vault includes the log bundle from every node in the cluster. Otherwise Cryptographic Security Platform Vault only includes the log bundle from the current node.
Include Core Files?	If selected, Cryptographic Security Platform Vault includes core files in the bundle.
Use a Passphrase to Encrypt the Bundle?	If selected, Cryptographic Security Platform Vault encrypts the bundle with an AES 256-bit key using the provided passphrase. Cryptographic Security Platform Vault will prompt you for the passphrase as soon as you press Enter.

When you press Enter, Cryptographic Security Platform Vault creates the bundle using the options you selected.

4. When you see the prompt that says the log bundle was successfully created, press **Enter**.
   If the Cryptographic Security Platform Vault webGUI is not available, please use the restricted shell to download the support bundle. For more information, see Using the Restricted Shell.
   You can also download the log bundle from the Cryptographic Security Platform Vault webGUI by selecting **Settings > Support > Download Logs**.

Note: If you want to decrypt the log bundle, navigate to the directory where the bundle is located and type the following command:

gpg -d -o <output-file-name> <input-file-name>

Where `<output-file-name>` is the name you want to use for the decrypted log bundle and `<input-file-name>` is the name of the encrypted log bundle that you want to decrypt.

Disabling CSP Vault Support Logins

Cryptographic Security Platform Vault support logins are automatically disabled 24 hours after being created. This procedure describes how to manually disable a support log in before that time has expired.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts** and press **Enter**.
3. On the Manage Accounts page, select the account you want to disable and press **Enter**.
4. The confirmation page shows the account name and when the password will automatically expire. To disable the account immediately, make sure **Yes** is selected and press **Enter**.
   Cryptographic Security Platform Vault disables the support account and returns to the main menu.

Policy Agent Support Logs

The Policy Agent logs information to the following files on Linux and Windows:

Linux— `/var/log/hcl.log`

Windows— `C:\Program Files\hcs\hcl.log`

To generate a log bundle containing pertinent system information, use the `hcsinfo` command. For details, contact Entrust Support.

Backing Up the Policy Agent

If you want to backup an the Policy Agent on an encrypted disk, you need to make sure the entire disk is backed up (for example, the entire VMDK file in a VMware vSphere environment). This ensures that the Entrust GUIDs representing the keys are also backed up so the data can be decrypted if it is restored from the backup. Once the backup is reauthorized with Cryptographic Security Platform Vault, Cryptographic Security Platform Vault can use the restored GUIDs to determine which keys apply to the restored data.

To create the backup, see your hypervisor documentation. Entrust does not provide any tools for backing up a VM.

Warning: Before you back up your VM, make sure you check the expiration date for the data encryption keys on the disk. If you restore a backup with expired keys and the expiration option is set to SHRED, Cryptographic Security Platform Vault will destroy the keys immediately and the data will be inaccessible. If you set the expiration option to NO USE, the keys can be reactivated after the back up is restored. For more information, see Encrypting a Disk Using the CLI.

Uninstalling the Policy Agent on Linux

Before You Begin

This procedure requires that you have a copy of the Policy Agent installer in your current directory. If this is not there, download the installer before you begin.

If you are using the htcrypt driver, you must uninstall it before you begin. For more information, see Uninstalling the HTCrypt Driver.

The Policy Agent can be uninstalled using the `/opt/hcs/bin/uninstall.sh` script. As part of uninstallation, all the binaries and configuration files will be removed. The encrypted block devices can no longer be decrypted after uninstalling the Policy Agent which will result in data loss. The Policy Agent can be uninstalled only after all root (system) devices are unencrypted, and the online encryption driver is removed. For more information, see Uninstalling the HTCrypt Driver.

Procedure

1. Decrypt all encrypted disks in the VM and remove the VM from the Cryptographic Security Platform Vault for VM Encryption as described in Decrypting a Disk Using the webGUI and Removing a VM from the Cryptographic Security Platform Vault for VM Encryption.
   Important: If you uninstall the Policy Agent without decrypting the disks, all access to the encrypted files will be lost because the encryption keys are deleted during the uninstall procedure.
2. Make sure that the Policy Agent can be uninstalled on the VM. To do so, expand the VM in the webGUI and look at the **Policy Agent Uninstallation Allowed** field on the **Details** tab. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

Tip: If you want to uninstall the Policy Agent from multiple VMs in this Cloud VM Set, you can change this property at the Cloud VM Set level and propagate the change to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.

3. Log into the VM as `root`.
4. Run the shell command `hcs-client-agent-10.5.3-build.number.run uninstall`. For example:

```
# sh hcs-client-agent-10.5.3-12345.run uninstall
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
Data on all encrypted volumes will be lost. Proceed with uninstall? (yes/no) yes
Encrypted device /dev/sdb1 detached; decrypted contents no longer visible
Encrypted device /dev/sdc1 detached; decrypted contents no longer visible
Encrypted device /dev/sdd1 detached; decrypted contents no longer visible
Stopping hcld... done
Uninstall successful
```

Uninstalling the Policy Agent on Windows

Before You Begin

This procedure requires that you have a copy of the Policy Agent installer in your current directory. If this is not there, download the installer before you begin.

If you are using the htcrypt driver, you must uninstall it before you begin. For more information, see Uninstalling the HTCrypt Driver.

The Policy Agent can be uninstalled using the `/opt/hcs/bin/uninstall.sh` script. As part of uninstallation, all the binaries and configuration files will be removed. The encrypted block devices can no longer be decrypted after uninstalling the Policy Agent which will result in data loss. The Policy Agent can be uninstalled only after all root (system) devices are unencrypted, and the online encryption driver is removed. For more information, see Uninstalling the HTCrypt Driver.

Procedure

1. Decrypt all encrypted disks in the VM and remove the VM from the Cryptographic Security Platform Vault for VM Encryption as described in Decrypting a Disk Using the webGUI and Removing a VM from the Cryptographic Security Platform Vault for VM Encryption.
   Important: If you uninstall the Policy Agent without decrypting the disks, all access to the encrypted files will be lost because the encryption keys are deleted during the uninstall procedure.
2. Make sure that the Policy Agent can be uninstalled on the VM. To do so, expand the VM in the webGUI and look at the **Policy Agent Uninstallation Allowed** field on the **Details** tab. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.
   Tip: If you want to uninstall the Policy Agent from multiple VMs in this Cloud VM Set, you can change this property at the Cloud VM Set level and propagate the change to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.
3. Log into the VM as `root`.
4. Run the shell command `hcs-client-agent-10.5.3-build.number.run uninstall`. For example:

```
# sh hcs-client-agent-10.5.3-12345.run uninstall
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
Data on all encrypted volumes will be lost. Proceed with uninstall? (yes/no) yes
Encrypted device /dev/sdb1 detached; decrypted contents no longer visible
```

```
Encrypted device /dev/sdc1 detached; decrypted contents no longer visible
Encrypted device /dev/sdd1 detached; decrypted contents no longer visible
Stopping hcld... done
Uninstall successful
```

KMIP Errors and Troubleshooting

KMIP Server Logs

- `/host/var/log/hcs/kmipsrv.log` : Transactions for server stop and start. This is mostly for debugging.
- `/host/var/log/hcs/traffic.log` : Fully-formatted KMIP protocol output. Key values are redacted.
- **Audit log**: You can configure the KMIP server to record all KMIP requests and responses or just the create/get requests and responses in the Cryptographic Security Platform Vault Audit log. You can also configure the server so that it does not log any KMIP information in the Audit log.

Troubleshooting

The most common errors are:

- Error 10 KMIP_ERROR_IO—Generally, the client is not talking to the server at all. This could be because of firewall issues, incorrect “Host Name” in KMIP client settings, or some other network issue. You can check connectivity with netcat via the console menu under “Diagnostic Tools”.
- Error 29 KMIP_ERROR_SSL_PARAMS—Seen when incomplete parameters are entered on the KMIP **Basic** tab.
- Error 30 KMIP_ERROR_SSL_PEER_VALIDATION—Seen when the KMIP server required Server Cert and one was not provided.
- Error 31 KMIP_ERROR_BAD_PASSWORD—One of the passwords entered for a KMIP client is incorrect.
- Error 32 KMIP_ERROR_BAD_TRUSTED_FILE—The CA cert argument specified for the KMIP client is incorrect.

Revert to Previous CSP Vault Version

When you upgrade to a newer version, Cryptographic Security Platform Vault automatically creates a pre-upgrade snapshot. Cryptographic Security Platform Vault allows you to revert to this previous version.

Important: If you have deleted the pre-upgrade snapshots, you cannot revert your upgrade to the previous installed version.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. On the Account Settings page, select System Upgrade.
   On the System Upgrade page, the previous upgrade version is displayed at the top in a yellow box.
   "A previous version <version number> is available to revert to."
5. Click the link on the text that says "revert to".
6. Click **Revert Upgrade**.
7. In the confirmation box, click **Proceed**.
8. Click **Reboot**.
9. In the confirmation box, click **Proceed**.

Cryptographic Security Platform Vault reverts to the previous upgrade.

Delete CSP Vault Snapshots

Cryptographic Security Platform Vault automatically creates a pre-upgrade snapshot whenever you upgrade to a newer version of Cryptographic Security Platform Vault. If you plan to increase your VM storage, you must delete any snapshots first.

Important: If you delete the pre-upgrade snapshots, you cannot revert your upgrade to the previous installed version. See Revert to Previous CSP Vault Version.

1. Log into the Cryptographic Security Platform Vault VM console as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Cryptographic Security Platform Vault Node**.
3. In the Manage the Cryptographic Security Platform Vault Node page, select **Delete** Cryptographic Security Platform Vault **pre-upgrade snapshot**.
4. In the confirmation screen, select **Yes**.

The snapshot is deleted, and there will be an audit message when it is complete.

Troubleshooting CSP Platform Vault from the Bootloader

If CSP Vault requires master key recovery or if the startup passphrase is set, then admin input is required during boot to unlock the root volume. When this happens, the Cryptographic Security Platform Vault webGUI displays the System Recovery dialog box, which is similar to the System Recovery Options dialog box. For more details, see Recovering Access to Cryptographic Security Platform Vault

If you cannot recover your system, then you need to use the Cryptographic Security Platform Vault Bootloader System Console to troubleshoot your issues. You can access the Bootloader System Console from either the Cryptographic Security Platform Vault VM console or by using an SSH connection to your Cryptographic Security Platform Vault IP address. You must log in as htadmin.

Note: If you log in using the VM console, you will see the following text. Enter y to start the System Console.

```
Please recover Cryptographic Security Platform Vault System Keys from WebGUI.
Cryptographic Security Platform Vault System Keys are not accessible.
Do you want to start KeyControl System Console? (y/n): y
```

Important: If you access the System Console using the VM console, and then successfully recover your system, you must quit the TUI before the VM boot will proceed. This does not apply if you access the System Console over SSH.

After you have logged in, you will see the following:

Option	Name	Description
1	Show HT encryption log file	Displays the log generated during boot for encryption or rekey. Run this command if requested by Support.
2	Set htsupport password	Enable the full support login account (`htsupport`). Enter the password and then confirm the password to enable.
3	Show Active network	Displays the active network addresses and routes for your Cryptographic Security Platform Vault node. If you set a temporary network, it displays the information for the new network.
4	Show persistent Cryptographic Security Platform Vault network	Displays the network configuration parameters currently configured for your Cryptographic Security Platform Vault node. This includes IP address, netmask, gateway, DNS address, and domain name.
5	Activate persistent Cryptographic Security Platform Vault network	Automatically restarts the Cryptographic Security Platform Vault networking service using the persistent network parameters.
6	Configure temporary network	Create a temporary network for your Cryptographic Security Platform Vault node. This command prompts for the network interface name, IP address, netmask, gateway, DNS address, and domain name. You can also enable DHCP.
7	Quit TUI Session	Close the System Console and return to the prompt.

Recovering Access to CSP Vault

There are times when you will need to recover your Cryptographic Security Platform Vault system, such as when you increase the number of CPUs allotted to a Cryptographic Security Platform Vault server, change the network hardware address, migrate Cryptographic Security Platform Vault to a different host, or restore from a backup to a newly-created VM. The system recovery process prevents rogue administrators from making unauthorized changes to, or copies of, Cryptographic Security Platform Vault disks.

- When you make a change that affects the hardware signature, the Cryptographic Security Platform Vault webGUI displays the **System Recovery** dialog box.

- For backup/restore, the Cryptographic Security Platform Vault webGUI displays the **System Recovery Options** dialog box.

Procedure

1. Select the method you want to use to recover your system. The options are:

Option	Description
Recovery using Keypart Upload	Allows you to upload the minimum number of required Admin Key parts that were sent to the Security Admins in the system. If you select this option, the webGUI displays the Recover Admin Key page. To upload a part, click Browse and select the appropriate `recovery_key` file. The Browse button should change to show the name of the selected file. When the correct file is displayed, click Upload file. Make sure that all Admin Key parts you upload have the same generation count. This information can be found in the email accompanying the Admin Key part. For details, see Admin Keys. When the required number of parts have been uploaded, Cryptographic Security Platform Vault recovers the system and displays the Recovery Success message. Click Proceed to return to the Cryptographic Security Platform Vault login page.
Recovery using Passphrase	Allows you to recover your system when you are using passphrase-based authentication. If you select this option, the webGUI displays the Recovery Passphrase page. Enter your passphrase and click Recover. For more information, see Startup Authentication.
Recovery from KMIP Server	Allows you to get an Admin Key stored on a KMIP server. The Admin Key must already be stored on this server for this option to work.
Recovery from HSM Server	Allows you to get the Admin Key from an HSM server. The Admin Key must already be stored on the HSM server for this option to work. If you select this option, the webGUI displays the HSM Recovery page where you can specify the following: • Partition Label, HA Group Name, or SoftCard Name • Partition, Crypto Officer (CO) password, or SoftCard password
Decommission	If you want to decommission your Cryptographic Security Platform Vault system, see Decommissioning a Cryptographic Security Platform Vault Node.

2. If there are multiple Cryptographic Security Platform Vault nodes in the cluster, re-join those nodes with the node you just recovered. For details, see Joining or Re-joining a Cryptographic Security Platform Vault Cluster.

CSP Vault Management webGUI Page Reference

- Alerts Page
- Audit Log Page

- Cluster Page
- HSM Server Settings Page
- Proxy Settings
- Users Page
- Settings Page
- SNMP Settings Page
- License Page
- Syslog Server Settings Page
- System Decommission Page
- System Upgrade Page

Alerts Page

The Alerts page gives you a quick overview of the major events that have taken place in the system. webGUI users can delete an alert from their local view, but the same alert will still be visible to other Cryptographic Security Platform Vault users. For more information, see CSP Vault Activity Tracking

To copy an alert to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple alerts, click the Multi-Select button and then left-click on the alerts you want to select.

To filter the alert list:

1. In the **Filter** drop-down list, select the field you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search tips for the available field types:

- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the alert was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.

Deleting Alerts

To delete one or more alerts from your local view:

1. Select the alerts you want to delete.
2. Select **Actions > Delete Alerts**.

Audit Log Page

Cryptographic Security Platform Vault tracks all activity on the system in the audit log. Users can export the audit log from the Cryptographic Security Platform Vault Management webGUI but they cannot change it in any way. For security reasons, Cryptographic Security Platform Vault tracks most of the events in the system.

> Note: You can also view the audit logs for each individual vault. The individual vaults do not support syslog and SNMP for audit logs.

For details, see:

- Cryptographic Security Platform Vault Activity Tracking
- Viewing the Audit Log
- Configuring Audit Log Settings
- Exporting the Audit Log

Cluster Page

The Cluster page contains the Cluster and Servers tabs, which show the health and basic configuration settings for the Cryptographic Security Platform Vault cluster as well as the connection status of all Cryptographic Security Platform Vault nodes in the cluster.

Cluster Tab

This tab displays the general health of the cluster as well as the basic configuration settings. It also allows you to join an existing cluster, add a new node to this cluster, backup your Cryptographic Security Platform Vault settings, or restore your settings from a previously-saved backup file.

For details, see:

- Cryptographic Security Platform Vault Nodes and Clusters
- Viewing the Cluster Status
- Setting Cluster Options
- Cryptographic Security Platform Vault Backup and Restore

Servers Tab

This tab includes one entry for each Cryptographic Security Platform Vault node in the cluster. For each node you can view or change the SSL certificate, reboot the node, or remove the node from the cluster.

For details, see:

- Removing a Cryptographic Security Platform Vault Node from a Cluster
- Joining or Re-joining a Cryptographic Security Platform Vault Cluster
- Changing the IP Address for a Node
- Rebooting a Cryptographic Security Platform Vault Node
- Cryptographic Security Platform Vault Certificates

HSM Server Settings Page

This page lets you configure the connection settings between Cryptographic Security Platform Vault and an Entrust or third-party Hardware Security Module (HSM).

An HSM is a physical server or PCI card that stores, protects, and manages cryptographic material. An HSM is often used to do cryptographic processing as well, including the generation of secure cryptographic keys. It is used in a client-server environment, which means that the server and the client each need to be prepared in advance. As with KMIP, the advantage of an HSM is that it protects and stores critical data such as your Admin Key and any Key Encryption Keys (KEKs) you have created for your Cloud VM Sets.

For details, see:

- Hardware Security Modules with CSP Vault
- Configuring Cryptographic Security Platform Vault as an HSM Client using an nShield HSM
- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding HSM Root-of-Trust to nShield Server
- Configuring Allowed Smart Cards for an nShield HSM
- Configuring an nShield HSM for High Availability
- Replacing an nShield HSM on a Cryptographic Security Platform Vault Cluster
- Configuring Cryptographic Security Platform Vault as a Luna HSM Client with a Single Cluster Certificate
- Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration
- Resetting the HSM Server Configuration
- Admin Keys
- KEKs with Cloud VM Sets

Proxy Settings

The Users page contains the Users tab, which shows all Cryptographic Security Platform Vault users configured in the system.

Cryptographic Security Platform Vault Managed Users Tab

You can create user accounts for Cryptographic Security Platform Vault that have access to certain areas of the Cryptographic Security Platform Vault webGUI based on their assigned user role. These accounts can also be used in the Entrust CLI (Command Line Interface) and the Entrust API calls when Cryptographic Security Platform Vault authorization is required.

For details, see:

- Cryptographic Security Platform Vault Authentication and User Accounts
- Authentication for Cryptographic Security Platform Vault User Accounts
- Setting the Cryptographic Security Platform Vault Management webGUI Session Timeout
- Creating a New Cryptographic Security Platform Vault-Managed User Account
- Setting webGUI User Preferences
- Changing Your Cryptographic Security Platform Vault User Account Settings
- About Two-Factor Authentication
- Changing Cryptographic Security Platform Vault Account Details as a Security Administrator
- Re-enabling a Cryptographic Security Platform Vault-Managed User Account

Users Page

The Users page contains the Users tab, which shows all Cryptographic Security Platform Vault users configured in the system.

Cryptographic Security Platform Vault Managed Users Tab

You can create user accounts for Cryptographic Security Platform Vault that have access to certain areas of the Cryptographic Security Platform Vault webGUI based on their assigned user role. These accounts can also be used in the Entrust CLI (Command Line Interface) and the Entrust API calls when Cryptographic Security Platform Vault authorization is required.

For details, see:

- Cryptographic Security Platform Vault Authentication and User Accounts
- Authentication for Cryptographic Security Platform Vault User Accounts
- Setting the Cryptographic Security Platform Vault Management webGUI Session Timeout
- Creating a New Cryptographic Security Platform Vault-Managed User Account
- Setting webGUI User Preferences
- Changing Your Cryptographic Security Platform Vault User Account Settings
- About Two-Factor Authentication
- Changing Cryptographic Security Platform Vault Account Details as a Security Administrator
- Re-enabling a Cryptographic Security Platform Vault-Managed User Account

Settings Page

The Settings page contains various sections that let you configure Cryptographic Security Platform Vault user account information, general configuration options, system settings, Cloud VM Set default settings, group SNMP settings, and Support options.

> Note: The sections and options displayed on this page depend on the privileges associates with your Cryptographic Security Platform Vault user account. If you cannot see an option that you want to set, contact your Cryptographic Security Platform Vault System Administrator.

Account Settings Section

This section lets you change your Cryptographic Security Platform Vault user account information, and, if applicable, download your portion of the Cryptographic Security Platform Vault Admin Key.

For details, see:

- Changing Your CSP Vault User Account Settings
- Admin Keys
- Downloading Your Admin Key Part
- About Two-Factor Authentication

  Note: If you have Security Admin privileges and you want to change the Cryptographic Security Platform Vault account details for a different user account, see Changing CSP Vault Account Details as a Security Administrator.

General Section

This section lets you configure general server settings and set the defaults for new Cryptographic Security Platform Vault user accounts.

For details, see:

- Authentication for CSP Vault User Accounts
  - Configuring Local Authentication Settings
  - Specifying an LDAP/AD Authentication Server
  - Specifying an OpenLDAP Authentication Server
  - Configuring an OpenID Connect Provider
- Connecting a CSP Vault to CSP Compliance Manager
- Admin Keys
- Configuring Audit Log Settings
- Setting the Default Account Expiration
- Setting Email Server Preferences
- Setting the CSP Vault Management webGUI Session Timeout
- Configuring TLS
- Uploading an OIDC CA Certificate

System Settings Section

This section lets you specify external connection information as well as upgrade, roll back, or decommission the system.

For details, see:

- Hardware Security Modules with CSP Vault
- Enabling an HTTP Proxy Server in CSP Vault
- SNMP Traps in Cryptographic Security Platform Vault
- Decommissioning a CSP Vault Node
- Configuring Syslog Server Settings
- Managing Two-Factor Authentication
- Setting CSP Vault Console Settings
- Setting CSP Vault Management webGUI Alert Settings

Cloud Settings Section

This section lets you specify the defaults you want to Cryptographic Security Platform Vault to use when you create a Cloud VM Set.

For details, see Setting Default Cloud VM Set Properties.

Support Section

This section lets you create a log bundle and then download that bundle so you can send it to Entrust.

For details, see:

- Support Access and Log Files
- Creating a Support Bundle with the webGUI

Group Settings Section

This section lets you configure SNMP for group-level alerts.

For details, see:

- SNMP Traps in Cryptographic Security Platform Vault
- Configuring Group-Level SNMP Traps

SNMP Settings Page

This page lets you configure your SNMP server connection for system-level alerts. This connection information will also be used for group-level alerts if no specific group-level connection information has been configured for this Cryptographic Security Platform Vault cluster.

You can also download the Cryptographic Security Platform Vault MIB file from this page.

For details, see:

License Page

Your Cryptographic Security Platform Vault license determines the number of nodes you can have in a cluster, the number of VMs that you can manage, and the length of time for which you can use the Cryptographic Security Platform Vault. Detailed license information is available in the Cryptographic Security Platform Compliance Manager, but you can view the status and the last time you have synced your Vaults and CSP Compliance Manager on the License page.

Several audit messages also contain information about your licenses for the CSP Vault for VM Encryption, the CSP Vault for Databases, the CSP Vault for Cloud Keys, and the CSP Vault appliance. For example:

- When you first upgrade from CSP Vault 10.4.x to 10.5.x, there is a 30-day upgrade grace period to get used to the new licensing model. The audit message informs you that you are in the grace period after upgrade, and that your system will become unlicensed when the grace period ends.
- When your CSP Vault is no longer connected to the CSP Compliance Manager, you will see a message saying that it has not synced to CSP Compliance Manager in x days. These messages start at 7 days after the last sync until the 30 day license sync grace period ends.

Beginning with 10.5.3, when there are important issues with your license, you will now see pop-up warnings in the Cryptographic Security Platform Vault webGUI as well as audit messages.

Syslog Server Settings Page

The Syslog Server Settings page allows you to view the settings of your Syslog Server, or enable or disable the server. When enabled, you can set the protocol to TCP or UDP, set the type of TLS authentication, the log format (RFC 5424 or CEF), and enter a list of syslog servers and their corresponding ports. You can also generate a certificate signing request, and, if required by your authentication mode, upload a CA certificate or client certificate. You can also reset the Syslog Server settings to the default values.

For details, see:

- Configuring Syslog Server Settings

- Resetting Syslog Server Settings

System Decommission Page

This page lets you decommission a Cryptographic Security Platform Vault node. When you decommission the node, Cryptographic Security Platform Vault zeroizes its disks and shuts down the node. If you want to decommission all nodes in a cluster, please decommission each node individually.

Warning: This is an irreversible procedure that could result in data loss if this is the only Cryptographic Security Platform Vault node in your system. If it is, make sure you have decrypted all disks registered with Cryptographic Security Platform Vault before you decommission the node or you will be unable to access the encrypted data after Cryptographic Security Platform Vault destroys the encryption keys.

For details, see Decommissioning a CSP Vault Node.

If you want to decommission a VM, see Decommissioning and Destroying a VM.

System Upgrade Page

This page displays the version of Cryptographic Security Platform Vault that you are currently running and gives you the option of upgrading the software or rolling it back to the previous version.

12 Vault Management

Vault Management Overview

CSP Vault administrators create vaults and assign a vault administrator to each vault. All configured vaults are shown on the Vault Management dashboard in the CSP Vault Management webGUI.

> Note: The CSP Vault Management webGUI has a session timeout value of 15 minutes. This cannot be changed.

The vault administrator configures and manages the vault. CSP Vault administrators do not have access to the vaults. For more information, see Managing Vaults.

For more information on managing each vault type, see:

- CSP Vault for Cryptographic APIs
- CSP Vault for CloudKeys
- CSP Vault for Databases
- CSP Vault for KMIP
- CSP Vault for Secrets
- CSP Vault for VM Encryption

Managing Vaults

CSP Vault administrators create vaults and the configured vaults are shown on the Vault Management dashboard.

For each new vault, the CSP Vault administrator specifies the vault type, vault name, and the vault administrator. See Creating a Vault.

The vault administrator is sent the details needed to access and configure the vault, including the vault security and policies.

If a vault administrator gets locked out of a vault, the CSP Vault administrator can 'rescue' the vault, allowing the vault administrator to log back into the vault using local credentials. See Rescuing a Vault.

Creating a Vault

CSP Vault security administrators create vaults and assign an administrator to each vault.

The vault administrator is sent the URL and a temporary password, allowing them to access and configure the vault. The vault administrator is responsible for the vault and has full control. Vaults are automatically created with local authentication. The vault administrator can change this at any time.

The Cryptographic Security Platform Vault administrator does not have access to the vault by default.

To create a vault

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Select **Create Vault**. The Create Vault page appears.
3. Enter the vault details:

Field	Description
Type	Select the vault type.
Name	Enter the name for the vault.
Description	Optional: Enter a description for the vault.
Email Notifications	Select ON or OFF to enable email notifications. If SNTP is not configured, email cannot be used. • If email is turned on, then an email is sent to the vault administrator. The email provides the URL of the vault and a temporary password. The vault administrator logs on to the vault with the tempory password and is prompted to change their password. • If email is turned off, then you will see and need to give the temporary passwords to the Vault Admins.
Admin Name	Enter the name of the vault administrator.
Admin Email	Enter the email address of the vault administrator. An email is sent to this email address, inviting the vault administrator to configure and manage the vault.

4. Select **Create Vault**.

Rescuing a Vault

If a vault administrator is locked out of a vault, the CSP Vault administrator can Rescue the vault.

Rescuing a vault resets the vault authentication to local authentication. Each vault administrator is sent an email with a new temporary password. They can then log on to the vault using the temporary password and reconfigure the vault.

Important: If two-factor authentication is enforced for the vault, then the user will need to add the one time password after the temporary password.

To rescue a vault

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.

3. In the Rescue Vault section, select **Rescue**.
   You are asked to confirm that you want to continue as rescuing the vault resets authentication to local authentication.
4. Select **Yes, Reset Authentication**.

The vault authentication is reset and a confirmation message appears.

An email is sent to vault administrators confirming that the vault has been rescued. The email includes a new temporary password to use to sign in to the vault.

Editing a Vault

You can change the vault name or description for a vault.

To edit a vault

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. Edit the vault name and/or description.
4. Select **Apply**.

The vault details are updated and a confirmation message appears.

Viewing Vault Details

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and click **View Details**.
   The Vault Details window displays the following information:
   - The name of the vault.
   - The type of vault.
   - The date that the vault was created.
   - The URL for the vault.
   - The URL for the Vault API.
   - The administrator name and user name.
3. Click **Close**.

Renaming a Vault

You can change the name of a CSP Vault after it has been created.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. In the Name field, update the name.
4. Click **Apply**.
5. Log into the Cryptographic Security Platform Vault for whose name you just changed.

The updated name should display in the top right of the CSP Vault Management webGUI. If the old name still appears, log out of the CSP Vault and log back in again.

Deleting a Vault

If a vault is no longer required, you can delete the vault and remove it from the vault management dashboard.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. Select **Delete Vault**.
   You are asked to confirm that you want to delete the vault.
4. Select **Yes, Delete**.

The vault is deleted and a confirmation message appears.

Connecting CSP Vault and CSP Compliance Manager

When you connect your CSP Vault to CSP Compliance Manager, the licensing for this vault will be tracked and maintained through Compliance Manager.

You will need to connect each vault that you have created to CSP Compliance Manager by importing a token file that was downloaded in Compliance Manager. The token file will be supplied by your CSP Compliance Manager administrator.

If you are also the administrator for CSP Compliance Manager, perform the tasks in Initializing a Data Source Connection in CSP Compliance Manager.

If you are not the admin for Cryptographic Security Platform Compliance Manager, request the Compliance Manager Token from the administrator and perform the tasks in Connecting a CSP Vault to CSP Compliance Manager.

- Initializing a Data Source Connection in CSP Compliance Manager
- Connecting a CSP Vault to CSP Compliance Manager
- Disconnecting a CSP Vault from CSP Compliance Manager

Initializing a Data Source Connection in CSP Compliance Manager

If you are the admin for CSP Compliance Manager, you will need to download the CSP Compliance Manager token file in CSP Compliance Manager and upload it into your CSP Vault.

1. Log into your Cryptographic Security Platform Compliance Manager webGUI.
2. In the side bar, click **Data Sources**.
3. Select **Actions > Initialize Connection**.
4. On the Initialize Connection to a Data Source page, enter the URL for the data source that you want to ad
5. Click **Create and Download File**.
   The Cryptographic Security Platform Compliance Manager downloads a file in .JSON format that will be used to connect to your data source.
   Important: This file should be considered a password. Please save it in a safe location in case you need to reconnect the same data source.

Connecting a CSP Vault to CSP Compliance Manager

After you have obtained the CSP Compliance Manager token file, you can upload it into your CSP Vault.

1. Log into your Cryptographic Security Platform Vault.
2. Click the **Settings** icon.
3. Click Cryptographic Security Platform Compliance Manager.
   Note: Alternatively, in the yellow 'This vault is not connected to Cryptographic Security Platform

Compliance Manager' area on the Home page, click **Connect Now** to be taken directly to the Cryptographic Security Platform Compliance Manager page.
4. On the Connect Cryptographic Security Platform Compliance Manager page, click **Connect**.
5. Upload the token file that you downloaded from the Cryptographic Security Platform Compliance Manager or received from the Cryptographic Security Platform Compliance Manager administrator.

Disconnecting a CSP Vault from CSP Compliance Manager

1. Log into your Cryptographic Security Platform Vault.
2. Click the **Settings** icon.
3. Click Cryptographic Security Platform Compliance Manager.
4. On the Cryptographic Security Platform Compliance Manager page, click **Disconnect**.
5. In the confirmation screen, click **Disconnect**.

13 CSP Vault Audit Messages 10.6.1

The Cryptographic Security Platform Vault audit messages are divided into four separate audit message files.

- The main audit file contains audit messages from the CSP Vault Management Appliance, the CSP Vault for Cloud Keys, the CSP Vault for Databases, and the CSP Vault for VM Encryption.
- The three smaller files contain audit messages from the CSP Vault for Cryptographic APIs, the CSP Vault for KMIP, and the CSP Vault for Secrets.

CSP Vault Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault Management Appliance, the Cryptographic Security Platform Vault for Cloud Keys, the Cryptographic Security Platform Vault for Databases, and the Cryptographic Security Platform Vault for VM Encryption.

There are many audit messages produced by Cryptographic Security Platform Vault. Many of these are informative and require no action. In the tabl below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a **%s** represents a string value. For example, in the following message:

  Added user **%s** to group **%s**

  The actual message will be displayed with the name of the user and group, for example:

  Added user **fred** to group **IT**

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
1	System License installed.	L	false	A new license has been uploaded and installed.		Security	Licensing
2	Begin System Initialization	L	false			Security	
3	Created group %s	M	false	The specified admin group has just been created.		Security	Account

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
4	Created Domain %s	L	false	This message appears during initialization of the first KeyControl node.		Security	Cluster
5	Added user %s to group %s	M	false	The user shown has been added to the specified admin group.		Security	Account
6	Expired password for user %s	H	false	A password has expired for the specified user.	The specified user needs to log into the GUI and change his/her password.	Security	Account
7	User %s logged out from ipaddr %s	L	false	The specified user has just logged out from the IP address shown.		Security	Account
8	Changed following attributes for user Security Administrator :- Password, Password Expiration Date, Password History List	M	false	One or more of the listed attributes has been changed for the user.		Security	Account
9	Changed SMTP Auth Settings	M	false	Email settings have been modified.		Security	Configuration
10	EKS has been removed, not destroying old admin keypair	M	false	Permission to use External Key Store has been removed. The old Admin Key was NOT removed on the EKS to allow restoration of older backups.	Informational only. Restore or add new access if so desired.	Security	EKS,KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
11	Regenerated Admin Key. The generation count of this key is %s. Reason: %s	H	true			Security	
12	Created Cloud VM Set %s	L	false			Security	
13	Could not create Cloud VM Set %s, HTCC server connection not configured	M	false			Security	Boundary Control
14	Masterkey Recovered on node %s	H	true			Security	
15	User %s logged in from ipaddr %s	L	false	The specified user has just logged in from the IP address shown.		Security	Account
16	Repeated login failures for %s from ipaddr %s	H	true	There have been a succession of login failures for the specified user.	A security admin should check whether the correct user has been trying to log in or not.	Security	Account
17	Account disabled for %s due to repeated login failures	H	true	The number of failed login attempts has reached the maximum allowed value.	A security admin needs to reset the account to enable access.	Security	Account
18	Server registration failed -- No license Installed	H	true			Security	Licensing

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
19	Attempt to register a new %s server "%s" failed -- licensed limit reached.	H	true	The number of KeyControl servers is already at the limit imposed by the license. An attempt is being made to another another node.	A new license will be required before the number of nodes in the cluster can be extended. Please contact hytrust.support@entrust.com	Security	Licensing
20	Storage Pool %s Filestore %s on server %s is low on space.	H	true			Clusters	
21	Changed following Settings :- %s	M	false			Security	
22	Changed following attributes for group %s :- %s	M	false	One or more of the listed attributes has been changed for the group shown.		Security	Account
23	Virtual Machine %s authenticated	L	false	A VM has registered or re-authenticated.	This message is in response to direct admin actions. No action is required.	Security	Reauth
24	Virtual Machine %s created in group %s	L	false			Security	
25	Removed Server %s from Cloud %s	L	false			Security	
26	Created Cluster Info %s	L	false			Security	
27	Removed Cluster Info %s	L	false			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
28	Activated account for user %s	M	false	A user's account has been activated.		Security	Account
29	Disabled account for user %s	H	false	A user's account has been disabled.	A security admin should check to see if the account should be enabled again.	Security	Account
30	Created user %s	M	false	The specified user has been created.		Security	Account
31	Deleted user %s	M	false	The specified user has been deleted.		Security	Account
32	Renamed user %s to %s	L	false	A username has been modified.		Security	Account
33	Deleted group %s	L	false	The specified groups has been deleted.		Security	Account
34	Renamed group %s to %s	L	false	An admin group has been renamed.		Security	Account
35	Removed user %s from group %s	M	false	The specified user has been removed from the group shown.		Security	Account
36	Using EKS for MasterKey protection	M	false	An External Key Store has been configured to protect the Admin Key.		Security	EKS,KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
37	Admin Key regeneration failed. Failed to use external KMIP Server for MasterKey protection	M	true	An External Key Store has been configured to protect the Admin Key but access was not allowed for keypair creation.	EKS denied access to create/retrieve an RSA keypair. Please check KMIP settings and configuration.	Security	EKS,KMIP
38	Could not register to HTCC, htcc server, password and login must be specified	H	false			Security	Boundary Control
39	Could not register to HTCC %s: HTCC login failed	H	false			Security	Boundary Control
40	Could not register to HTCC %s. Please check user privileges and Boundary Control License on HTCC	H	false			Security	Boundary Control
41	Successfully registered with HTCC Server %s	M	false			Security	Boundary Control
42	Keyid %s has %s	H	true	Keyid has expired and/or rotated. Keys only expire if a Cloud Admin has explicitly set them to expire.		Security	KeyID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
43	The Key for disk %s Virtual Machine %s has %s	H	true	A key for the specified VM has either expired or been rotated. Keys only expire or rotate if a Cloud Admin has explicitly set them to expire or rotate.		Security	KeyID
44	Key in VMSet %s on VMV %s has %s	M	true			Security	KeyID
45	Changed following KeyControl cluster settings :- %s	M	false	The name of the cluster has been modified.		Clusters	Domain
46	Deleted Domain %s	M	true			Security	Domain
47	Changed following KPS Settings :- %s	M	false			Security	Configuration
48	Changed following VS Appliance Settings :- %s	M	false			Security	
49	Unknown pool %s appeared on VMV, destroying...	M	true			Security	
50	Changed following Storage Pool Settings :- %s	M	false			Security	
51	Changed following attributes of filestore %s :- %s	M	false			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
52	Changed following settings for Cluster Info %s :- %s	M	false			Security	
53	Coretrace Server %s, changed following attributes :- %s	M	false			Security	CoreTrace
54	Changed following settings for Cloud VM Set %s :- %s	M	false			Security	
55	Cloud VM Set %s changed group ownership from %s to %s.	H	false			Security	
56	Deleted Cloud VM Set %s	M	false			Security	
57	Cloud VM Set %s: added keyid %s using %s cipher	H	false	A VM user has explicitly requested creation of a KeyID using the specified cipher.		Security	KeyID
58	Cloud VM Set %s: Virtual Machine %s removed keyid %s	M	false	A VM user has explicitly requested deletion of the specified KeyID. It has been removed from the specified Cloud VM.		Security	KeyID
59	Cloud VM Set %s: updated keyid %s	L	false	The KeyID description was changed.		Security	KeyID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
60	Cloud VM Set %s: Virtual Machine %s attempted to fetch inactive keyid %s	M	false	The KeyID shown has been revoked but an attempt was made to fetch it.	The cloud admin who owns the key should determine whether access should be reinstated or not.	Security	KeyID
61	Cloud VM Set %s: Virtual Machine %s attempted to fetch expired keyid %s	M	false	An attempt has been made to fetch an expired KeyID.	The cloud admin who owns the key should determine whether access should be reinstated or not. This is only possible if the KeyID was set to 'No use?' on expiration.	Security	KeyID
62	Cloud VM Set %s: Virtual Machine %s fetched keyid %s	M	false	A request has been made to access the specified KeyID.		Security	KeyID
63	Revoked permission for keyid %s	M	true	KeyID is currently revoked. It must be activated before use.	The cloud admin who owns the key should determine whether access should be reinstated or not.	Security	KeyID
64	Granted permission for keyid %s	H	true	KeyID has been activated after having been previously revoked.		Security	KeyID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
65	Cloud VM Set %s keyid %s updated - description %s	L	false	The description field for the specified KeyID has been updated.		Security	KeyID
66	Cloud VM Set %s keyid %s updated - key expires on %s, onexpiry %s	M	false	The expiration date and effect on expiration for the specified KeyID have been updated.		Security	KeyID
67	Cloud VM Set %s Keyid %s has expired	M	true	An expiration date has been hit for the specified KeyID	The owning cloud admin should verify that the KeyID should be no longer used.	Security	KeyID
68	Keyid %s has expired	M	true	A request to access an expired KeyID has been made.	The owning cloud admin should verify that the KeyID should be no longer used.	Security	KeyID
69	The Key for keyid %s in Cloud VM Set %s expires in %d day(s). Please extend the key life.	M	true	A KeyID is about to expire.	The owning cloud admin should verify that the KeyID should be expire and change the date if not.	Security	KeyID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
70	Unable to check keyid %s	M	false	An error occurred while attempting to check properties of KeyID.	An internal error occurred while checking expiration/ rotation properties for specific keyid. Informational only, keyid will be checked again.	Security	KeyID
71	Cloud VM Set %s: added fsid %s using %s cipher	M	false			Security	
72	Cloud VM Set %s: Virtual Machine %s removed fsid %s	M	false			Security	
73	Cloud VM Set %s: Virtual Machine %s updated fsid %s	M	false			Security	
74	Revoked permission for fsid %s	M	true			Security	
75	Granted permission for fsid %s	M	true			Security	
76	Cloud VM Set %s fsid %s updated - key expires on %s, onexpiry %s	M	false			Security	
77	Cloud VM Set %s Fsid %s has expired	M	true			Security	
78	Properties changed for VMSet %s on server %s (%s)	M	false			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
79	Virtual Machine %s, changed following attributes: %s	M	false			Security	
80	Deleted Virtual Machine %s	L	true			Security	
81	Deleted Certificate %s	L	false	An unused certificate was deleted		Security	
82	The Virtual Machine %s, could not be checked for geo-location boundary. HTCC login failed	H	true			Security	Boundary Control
83	The Virtual Machine %s, is not in the geo-location boundary. Key access is denied	H	true			Security	Boundary Control
84	The Virtual Machine %s, is in the geo-location boundary. Key access is granted	M	true			Security	Boundary Control
85	Added Virtual Machine %s, authentication complete	L	true	A VM has completed registration.	This message is in response to direct admin actions. No action is required.	Security	Reauth
86	Added Virtual Machine %s, authentication pending	M	true	A VM has a registration request pending.	The cloud admin needs to complete authentication in the KeyControl GUI.	Security	Reauth

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
87	Removed Server %s from Cloud %s	L	false			Security	
88	Renamed Server %s to %s	L	false			Security	
89	Virtual Machine %s re-connected, authentication pending	H	true	A VM has a re-authorization request pending.	The cloud admin needs to complete re-authorization in the KeyControl GUI.	Security	Reauth
90	Revoked permissions for Virtual Machine %s	M	false			Security	
91	Re-authenticated Virtual Machine %s from KPS	M	false	A VM has a re-authorized.	This message is in response to direct admin actions. No action is required.	Security	Reauth
92	Virtual Machine %s added disk %s	L	false	A new disk has been added to the specified VM.		Security	Key
93	Virtual Machine %s removed disk %s	L	true	A disk has been removed from the specified VM.		Security	Key
94	Virtual Machine %s : disk %s renamed to %s	L	false			Security	Key
95	Virtual Machine %s attempted to fetch key for inactive disk %s. %s	L	false	If a disk is not active, no keys will be delivered.		Security	Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
96	Virtual Machine %s attempted to fetch expired key for disk %s. %s	H	false	If a key has expired an attempt by a VM to fetch the key will fail.	The cloud admin should determine whether the expiration date should be extended. This does not apply to shredded keys.	Security	Key
97	Virtual Machine %s fetched key for disk %s. %s	L	false	A key for the specified disk has been requested by the VM shown.		Security	Key
98	Virtual Machine %s created key for disk %s using %s cipher	L	false	A disk has been encrypted. The type of cipher is shown.		Security	Key
99	Virtual Machine %s revoked permission for disk %s	M	true			Security	Key
100	Virtual Machine %s granted permission for disk %s	M	true			Security	Key
101	Virtual Machine %s added mount point %s	L	false	An encrypted folder has been mounted.		Security	Key
102	Virtual Machine %s removed fs %s	L	true	An encrypted folder has been removed.		Security	Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
103	Virtual Machine %s attempted to fetch key for inactive fsid %s	M	false	A virtual machine attempted to access an inactive FSID.	The cloud admin should determine whether the FSID should be made accessible.	Security	Key
104	Virtual Machine %s attempted to fetch expired key for fsid %s	H	false	The FSID has expired and therefore the filesystem cannot be mounted.	The cloud admin should determine whether the FSID should be made accessible. This is only possible if the FSID has not been shredded.	Security	Key
105	Virtual Machine %s fetched key for fsid %s	L	false	A filesystem was mounted using the specified FSID.		Security	Key
106	The Key for disk %s Virtual Machine %s has expired	H	true	An attempt is being made to change properties for an already expired key.	The cloud admin should determine whether the key of the disk should be made accessible. This is only possible if the disk's key has not been shredded.	Security	Key
107	Virtual Machine %s set key expiry to %s, onexpiry to %s for disk %s	H	false	An expiration date has been set on a key for the specified disk. The effect taken on expiration is shown.	The cloud admin should determine whether the expiration date should be extended.	Security	Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
108	The Certificate for Virtual Machine %s expire%s %d days%s. Please renew the certificate.	M	true			Security	
109	The Key for disk %s Virtual Machine %s has expired	H	true	The key shown for the specified VM has expired.	The cloud admin should determine whether the expiration date should be extended.	Security	Key
110	The Key for disk %s Virtual Machine %s expires in %d day(s). Please extend the key life.	H	true	The encryption key shown is about to expire.	The cloud admin should determine whether the expiration date should be extended.	Security	Key
111	Unable to check key for disk %s Virtual Machine %s	M	false	An error occurred while attempting to check properties of key for the given disk and VM.	An internal error occurred while checking expiration/ rotation properties for specified key. Informational only, key will be checked again.	Security	Key
112	Virtual Machine %s rebooted, reauthentication required	H	true	A VM has rebooted and the reboot setting requires that the VM is re-authenticated.	The cloud admin needs to complete re-authorization in the KeyControl GUI.	Security	Reauth
113	Virtual Machine %s has new alerts, please check	M	true			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
114	Added Coretrace policy "%s" to Virtual Machine %s	L	true			Security	CoreTrace
115	Activated Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
116	De-activated Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
117	Modified Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
118	Removed Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
119	Deleted CAStore %s	M	false			Security	
120	Removed Server %s from Domain %s	L	false			Clusters	Domain
121	Storage pool %s created on server %s (%s)	L	false			Security	
122	Storage pool %s extended on server %s (%s)	L	false			Security	
123	Log added to Storage pool %s on server %s (%s)	L	false			Security	
124	Log removed from Storage pool %s on server %s (%s)	L	false			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
125	Storage pool %s deleted from server %s (%s)	L	false			Security	
126	Disk added to hot spare list on server %s (%s)	L	false			Security	
127	Disk removed from hot spare list on server %s (%s)	L	false			Security	
128	Filestore %s created on server %s (%s)	L	false			Security	
129	Filestore %s deleted from server %s (%s)	L	false			Security	
130	Removed server %s (%s) from domain %s	L	true			Clusters	
131	KMIP Server restarted on %s	M	false	The KMIP server has been restarted on the specified host.		Security	KMIPServer
132	KMIP Server started on %s	L	true	The KMIP server has been started on the specified host.		Security	KMIPServer
133	KMIP Server halted on %s	H	true	The KMIP server has been halted on the specified host.		Security	KMIPServer
134	KMIP Server: All client certificates removed	H	true	All client certificates have been removed from the KMIP server.		Security	KMIPServer

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
135	KMIP Server: Client certificate %s removed	H	true	The specified client certificate has been removed from the KMIP server.		Security	KMIPServer
136	KMIP Server: Client certificate %s updated	M	false	The specified client certificate has been updated on the KMIP server.		Security	KMIPServer
137	KMIP Server: Client certificate %s created	M	true	The specified client certificate has been created on the KMIP server.		Security	KMIPServer
138	Could not store oskey on %s/%s. Needs recovery	H	true	Could not store object store key on joining KC node	KC join did not succeed, node should be removed from cluster. If problem persists contact support.	Clusters	HCAuth
139	Reconnect not allowed for %s/%s. Please follow reauthenication steps	H	true	KC has attempted to reauthenticate with cluster that does not recognize it	KC node likely was in the cluster and removed. Should be re-joined	Clusters	HCAuth
140	Cluster join failed for %s/%s.	H	true	KC has failed to join cluster	KC node join can be attempted again. If problem persists contact support	Clusters	HCAuth

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
141	Reconnect info does NOT match. Follow reauthentication steps for node %s/%s	H	true	KC has attempted to reauthenticate with cluster but its info has changed	KC node likely needs MasterKey recovery or kicked out of cluster and re-joined	Clusters	HCAuth
142	Could not store connection info for %s/%s	H	true	KC cannot store info to reconnect to cluster on restart	Condition could be transitory, node could be restarted. Also could indicate that KC disk is full	Clusters	HCAuth
143	Problem with auth/ secd communication	H	true	Communication stack on KC is not working		Clusters	HCAuth
144	System utilities NOT functioning. Authentication will not happen	H	true	Auth daemon unable to query system information		Clusters	HCAuth
145	Attempt to add node %s/%s which has valid data but no clusterid. Please reauthenticate if this is a valid action.	M	true	KC was formerly in a cluster that has no identifying cluster ID	If action is a valid one, proceed with join. Note that the KC data on joining node will be destroyed	Clusters	HCAuth
146	Attempt to add node %s/%s which has a different clusterid. Please reauthenticate if this is a valid action.	M	true	KC was formerly in a different cluster than the one it is attempting to join	If action is a valid one, proceed with join. Note that the KC data on joining node will be destroyed	Clusters	HCAuth

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
147	Could not restore cluster to normal operating mode after adding new node, error $rc	M	true	KC cluster state could not be restored to normal operating state	Can indicate cluster join issues	Clusters	HCAuth
148	KeyControl Server system `hostname` ($myip) $act.	L	false			Clusters	
149	Restricted support login enabled on `hostname`	M	true	Restricted support login was enabled on KC		Security	
150	%s support login enabled on `hostname`	M	true	Full or Restricted support login was enabled on KC		Security	
151	%s support login disabled on `hostname`	M	true	Full or Restricted support login were disabled on KC		Security	
152	KeyControl node {$myip[0]}/ {$myhost[0]} has failed upgrade to version {$curver}	H	true	KC upgrade to new version has failed	KC will revert to prior install. Upgrade can be attempted again if valid or contact support	Clusters	Upgrade
153	KeyControl node {$myip[0]}/ {$myhost[0]} reverted from {$str[1]} to {$str[2]}	M	true	User initiated revert to previous version has succeeded.		Clusters	Upgrade
154	KeyControl node {$myip[0]}/ {$myhost[0]} has successfully upgraded to version {$curver}	M	true	KC upgrade to new version has succeeded.		Clusters	Upgrade

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
155	KeyControl node {$myip[0]}/{$myhost[0]} has failed upgrade finalization to version {$curver}	H	true	KC upgrade to new version has failed	KC will revert to prior install. Upgrade can be attempted again if valid or contact support	Clusters	Upgrade
156	Hostname %s, Management IP %s, Current Version %s, New Version %s. Upgrade from version {$oldver} (b{$oldrevision}) to version {$curver} (b{$newrevision}) not allowed. Consult product documentation for upgrade procedure	H	true	KC upgrade to this version is not supported from current version	Upgrade to a supported version and/or contact support	Clusters	Upgrade
157	Upgrade from version {$oldver} to version {$curver} not officially supported but allowed for development	L	true	KC upgrade to this version is not officially supported but allowed for development build		Clusters	Upgrade
158	Internal error $ret checking upgrade from {$oldver} to {$curver}	H	true	An error has occurred attempting to valid upgrade	Contact support	Clusters	Upgrade
159	Multiple KeyControl nodes still in cluster. All excess KeyControl nodes must be removed before upgrade.	H	true	Upgrade should be attempted on only a single node cluster	Remove all nodes from cluster except the node to be upgraded	Clusters	Upgrade

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
160	Insufficient free space to perform upgrade. Consult product documentation for procedure to add another disk	H	true	Disk does not have enough space for upgrade	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade
161	System has reverted to prior installation.	L	true	System has successfully reverted to prior version		Clusters	Upgrade
162	Failed revert to prior installation.	H	true	System failed to revert to prior version	Contact support. Current version is still in place	Clusters	Upgrade
163	System utilities NOT functioning.	H	true	Unable to query system info		Clusters	
164	Error resizing partition	H	true	An error occurred while resizing the KeyControl storage. Please contact support.		Clusters	
165	Error resizing storage pool	H	true	An error occurred while resizing the KeyControl storage. Please contact support.		Clusters	
166	Successfully resized KeyControl storage pool	M	false	The storage pool on the KeyControl node was successfully resized.		Clusters	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
167	KMIP Server operation failed - internal error	M	true	KMIP server operation failed with an internal error.	Consult support or retry operation	Security	KMIPServer
168	%s operation %s for %s on %s, TaskId: %s.	L	false	A task has changed state		Security	
169	Virtual Machine %s : disk %s resized to %s	L	false	Virtual Machine disk is resized		Security	
170	Virtual Machine %s : KC mapping %s attached	L	false	A KC Mapping is attached to a VM		Security	
172	Passwd changed for htadmin	M	true	An admin reset console/htadmin passwd		Security	
173	User %s failed to change %s passwd	M	true	An admin attempted a reset console/htadmin passwd that failed		Security	
174	A support event has occurred on KeyControl node %s. Please create a Support Bundle as described in the online help, then contact support.	H	true	Please contact support for more information		Security	
175	New certificate created with guid %s in group %s	L	false	A new certificate has been create for use with policy agent or KMIP server		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
176	Backup created successfully for %s (%s)	L	false	A new backup image has been created on the KeyControl appliance		Clusters	
177	Failed to create backup for %s (%s)	M	false	Creation of the backup image failed.	Backup will be retried automatically or can be triggered manually via the WebGUI	Clusters	
178	KeyControl Cluster is in normal mode	L	false	The KeyControl cluster state has returned to normal operating mode		Clusters	
179	KeyControl Cluster is in degraded mode	H	false	The KeyControl cluster has gone into degraded mode. This occurs when the KeyControl nodes in the cluster are not able to communicate successfully	Check the availability and connectivity of the KeyControl nodes in the cluster	Clusters	
180	KeyControl Cluster is in standby mode	L	false	The KeyControl cluster is in a standby state. This is a temporary state which occurs when a node is joining the cluster		Clusters	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
181	Freespace available on %s has fallen below 2G. An upgrade to the storage for this system should be considered.	H	true	The amount of free disk space available to the KeyControl appliance has dropped below our recommended threshold. Please increase the size of the disk or contact support for more assistance	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	
182	Login failure for %s from %s	L	false	User unsuccessfully attempted to login to the KeyControl instance		Security	
183	Reboot of %s initiated by %s	M	true	Domain administrator initiated reboot of KeyControl node		Clusters	
184	KeyControl node reboot initiated from console	M	true	The KeyControl node was rebooted from the console		Security	
185	KeyControl node shutdown initiated from console	M	true	The KeyControl node was shutdown from the console		Security	
186	Azure agent: illegal attempt to install plugin	M	true	Azure "extensions" (a.k.a. "plugins") to a KeyControl VM are not allowed		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
187	Azure agent: illegal attempt to disable or uninstall a plugin	M	true	Azure "extensions" (a.k.a. "plugins") to a KeyControl VM are not allowed		Security	
188	%d inactive tasks found on Cloud VM Set %s. %s task for %s on %s not updated since %s, TaskId: %s.	L	true	List of tasks that have not been updated for a long time		Security	
189	Updated LDAP configuration: %s	M	false	The values for the given LDAP fields have been updated		Security	
190	Virtual Machine %s synchronized devices. Following devices were not found - %s	M	false	The Policy Agent synchronized the registered device list; some devices not found		Security	
191	Virtual Machine %s synchronized devices. Reason for sync: %s	M	true	The Policy Agent synchronized the registered device list		Security	
192	Virtual Machine %s state for disk %s changed to %s. %s	L	false	Disk state on policy agent changed		Security	
193	HyTrust bootloader ssh key updated for %s	L	false	Private key required for ssh login to hytrust bootloader updated on KC		Security	
194	Two-factor authentication enabled for %s	L	false	Two factor authentication has been enabled for the user		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
195	Two-factor authentication disabled for %s	M	true	Two factor authentication has been disabled for the user		Security	
196	KeyControl Cluster is in degraded mode during node-join	L	false	The KeyControl cluster has gone into degraded mode while a new node is joining the cluster. This occurs as KeyControl restarts communication protocols after a new node has joined the cluster.		Clusters	
197	KeyControl Cluster is in degraded mode during node-join	L	false	The KeyControl cluster has gone into normal mode while a new node is joining the cluster. This occurs as KeyControl restarts communication protocols after a new node has joined the cluster.		Clusters	
198	New AppLink created to %s	M	true	A new Application Link has been created. This link will allow secure communication between the Entrust products.		Clusters	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
199	Application link removed for Product (%s) Version (%s) IP List (%s)	L	false	Application link has been removed for the external product.		Clusters	
200	admin user logged in successfully	M	false	htadmin account login successful in one of the KeyControl nodes		Security	Support
201	%s account logged in from IP	M	false	Full support account login successful in one of the KeyControl nodes		Security	Support
202	htadmin account login failure	M	false	Failed attempt to login to htadmin account		Security	Support
203	%s account login failure from IP - Reason	M	false	Failed attempt to login to full support account		Security	Support
204	Full support account user logged in from IP and executed command	M	false	Full support account login successful and executed a command		Security	Support
205	%s account login failure from IP attempting command	M	false	Failed attempt to login to full support account and execute command		Security	Support
206	Created new log bundle - %s with options - %s	L	false	New log bundle creation has been initiated by some user		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
207	Downloaded log bundle - %s	L	false	Latest log bundle has been downloaded by some user		Security	
208	Exported Cloud VM Set %s	M	false	A Cloud VM Set has been exported		Security	
209	Imported Cloud VM Set %s	M	false	A Cloud VM Set has been imported		Security	
210	Following guests have unsupported policy agent installed in Cloud VM Set %s: %s(%s)	M	true	A Cloud VM Set has guests with unsupported agent version	Upgrade policy agent on reported guests	Security	
211	Unsupported Policy Agent (version %s) detected on guest %s.	M	false	A guests has unsupported agent version installed	Upgrade policy agent on reported guest	Security	
212	Download of admin key generation %s initiated by %s	M	false	Download of admin key initiated via admin_key GET call		Security	
213	Reset of KMIP server initiated	M	false	Reset of KMIP server initiated		Security	
214	KMIP Response/ Request: < op> <obj> <result>	M	false	Create, destroy or revoke of KMIP object initiated		Security	
215	KMIP Response/ Request: < op> <obj> <result>	M	false	Operation on some KMIP object initiated		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
216	The Certificate for Virtual Machine %s will auto-renew in %d days	L	true			Security	
217	The Certificate for Virtual Machine %s failed to auto-renew. Certificate expires %d days. Please renew the certificate.	H	true			Security	
218	Set Key Encryption Key expiry to %s on expiry to %s, for Cloud VM Set %s. %s Cloud VMs affected.	H	false	An expiration date has been set for Key Encryption Key for the specified Cloud VM Set. The effect taken on expiration is shown.	The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key
219	The Key Encryption Key for Cloud VM Set %s expire%s in %d days%s.	H	true		The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key
220	The Key Encryption Key for Cloud VM Set %s has expired. %s Cloud VMs affected.	H	true	The Key Encryption Key for specified Cloud VM Set has expired.	The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key
221	Access to Key Encryption Key of Cloud VM Set %s has been revoked. %s Cloud VMs affected.	H	true	Access to specified Cloud VM Set has been revoked.		Security	Key Encryption Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
222	Access to Key Encryption Key of Cloud VM Set %s has been granted. %s Cloud VMs affected.	H	true	Access to specified Cloud VM Set has been granted.		Security	Key Encryption Key
223	The Key Encryption Key for Cloud VM Set %s has expired. %s Cloud VMs deleted. Deleted CVM Set %s.	H	true	The Key Encryption Key for specified Cloud VM Set has expired.		Security	Key Encryption Key
224	The Certificate for Virtual Machine %s failed to auto-renew as the Virtual Machine is unreachable.	H	true	The Certificate Auto Renewal of a VM fails if the VM is in auto renewal period and is unreachable.		Security	
225	Authentication of Server %s (%s) failed due to incorrect passphrase		false	Authentication of KeyControl node failed due to incorrect passphrase.		Security	
226	Cloud VM Set creation failed. Error: Failed to store key in HSM. %s	H	true	Cloud VM Set creation failed. Failed to store key in HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key
227	Key Encryption Key import failed. Error: Failed to store key in HSM. %s	H	true	Key Encryption Key import failed. Failed to store key in HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
228	Failed to fetch Key Encryption Key from HSM. Error: %s	H	true	Failed to fetch Key Encryption Key from HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key
229	Successfully imported Key Encryption Key for Cloud VM Set %s.		false	Successfully imported Key Encryption Key		Security	Key Encryption Key
230	Removed Domain %s from group %s		false	Removed Domain from group		Security	
231	Authenticated Server %s (%s)		false	New Key Control has been successfully authenticated and added to the cluster		Clusters	
232	Added Server %s (%s) to Domain %s		false	Server has been successfully added to a domain		Clusters	
233	Invalid Key Encryption Key size specified for Cloud VM Set %s.	H	true	Invalid Key Encryption Key size	Verify that the Key Encryption Key size is 128 bits or 256 bits	Security	Key Encryption Key
234	Retention period has expired for Cloud VM Set %s. %s Cloud VMs deleted. Deleted Cloud VM Set %s.	L	true	Retention period has expired for Cloud VM Set		Security	Key Encryption Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
235	Retention period for Cloud VM Set %s will expire in %d days.	H	true	Retention period expiration for Cloud VM Set	The cloud admin should determine whether the retention date should be extended.	Security	Key Encryption Key
236	Set Retention Date to %s for Cloud VM Set %s.		false	Changed Retention period for Cloud VM Set		Security	Key Encryption Key
237	Failed to delete Key Encryption Key from HSM for Cloud VM Set %s. Error: %s.	M	true	Failed to delete Key Encryption Key from HSM		Security	Key Encryption Key
238	New CA Certificate added to Certificate Store for verifying %s		false	New CA certficate has been added to verify some subsystem		Clusters	
239	CA Certificate for %s removed from Certificate Store		false	CA Certificate for some subsystem has been removed from Certificate Store		Clusters	
240	Authentication for LDAP user %s failed. Reason :- %s		false	Reason for LDAP login failures		Security	
241	Cannot register Cloud VM until Key Encryption Key for Cloud VM Set %s is imported	L	true	Cannot register Cloud VM		Security	Key Encryption Key
242	Virtual Machine %s HTcrypt driver update -- %s	L	false	HTcrypt driver state on policy agent changed		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
243	New self-signed certificates generated for %s	L	false	New self-signed certificates generated for server		Clusters	Certificate
244	New SSL certificate installed for %s	L	false	New SSL certificate installed for server		Clusters	Certificate
245	CSR generated with common name - %s	L	false	New CSR generated		Clusters	Certificate
246	Web server for %s restarted	L	false	Webserver/ Apache restarted for server		Clusters	Certificate
247	Certificate installation task got timed out. There are VMs that did not receive the new CA certificate. Please contact Cloud Administrators to login to the VM and execute hcl heartbeat before restarting the webserver	H	true	One (or more) policy agents did not receive the new CA certificate uploaded. Cloud administrator has to login to the policy agent and execute hcl heartbeat		Clusters	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
248	Cannot update CA as part of SSL certificate installation for %s. Please login to the VM and execute hcl heartbeat	H	true	Domain Administrator has attempted to install a new SSL certificate for the webserver. Unfortunately one of the policy agents did not receive a copy of the new CA certificate that can verify the SSL certificate of the webserver. Cloud administrator has to login to the policy agent and execute hcl heartbeat		Clusters	Certificate
249	External web server certificate of %s has expired. A new certificate must be installed before the associated VMs can communicate with %s. After the new certificate has been installed, the certificate information on the associated VMs must be manually updated if the new certificate is from a different Certificate Authority. For more information, search for certificates in the WebGUI online help.	H	true	Certificate used by the external webserver of one of the nodes has expired. Domain administrator has to install a new certificate. If the newly installed certificate is generated by a new CA, cloud administrators will have to login to policy agent and update the CA certificate file. The latest CA certificate file can be found in the cloud tab in webGUI		Clusters	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
250	External web server certificate of %s will expire in %s days, %s hours and %s minutes. If another certificate is not installed before the current one expires, the VMs will not be able to communicate with %s after %s and all VMs may need to be manually updated after the new certificate is installed. For more information, search for certificates in the WebGUI online help.	H	true	Certificate used by the external webserver of one of the nodes is about to get expired. Domain administrator has to install a new certificate before it gets expired. Otherwise policy agents will not be able to communicate with the KC after expiry		Clusters	Certificate
251	CA certificate used for verifying %s:%s on %s has already expired. Please upload a new CA certificate to verify the %s server certificate. Otherwise %s users will not be able to login to the WebGUI.	H	true	CA certificate used by the LDAP server has already expired. Security Administrator has to install a new certificate to verify the LDAP server certificate. Otherwise LDAP users will not be able to login to the WebGUI.		Clusters	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
252	CA certificate used for verifying %s:%s on %s will expire in %s days, %s hours and %s minute. If another CA certificate is not installed before the current one expires, %s users will not be able to login to the WebGUI after %s.	M	true	CA certificate used for evaluating LDAP server certificate is about to get expired. Security Administrator has to install a new certificate before the current one expires. Otherwise LDAP users will not be able to login to the WebGUI after the CA certificate expiry date.		Clusters	Certificate
253	Certificate for %s:%s has already expired. Please re-configure %s after updating the certificate in %s.	H	true	Certificate for APPLINK has already expired. APPLINK should be reconfigured after uploading a new certificate.		Clusters	Certificate
254	Certificate for %s:%s will expire in %s days, %s hours and %s minutes. Once the certificate of %s is updated, please re-configure the %s:%s	M	true	Certificate for APPLINK is about to get expired. Security Administrator has to install a new certificate and re-configure the APPLINK before the current one expires.		Clusters	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
255	KeyControl Cluster is in maintenance mode	L	false	The KeyControl cluster is in maintenance state. This is a temporary state which occurs during upgrade process		Clusters	
256	Virtual Machine with IP %s is a possible clone of %s (%s) and hardware signature verification is turned off.	H	true	A possible clone of a Virtual Machine that is already registered has been detected. Verify that the VM is valid and register it as a new VM using 'hcl register -c' command.		Security	
257	KeyControl cluster has been successfully upgraded from KC %s to version KC %s	M	true	KeyControl cluster upgrade to new version has succeeded.		Clusters	Upgrade
258	KeyControl cluster has been successfully reverted from KC %s to version KC %s	M	true	KeyControl cluster revert to old version has succeeded		Clusters	Upgrade
259	Access Control Policy: %s, at version: %s applied to disk: %s on VM: %s	H	true	Access Controls Policy version update to disk.		Security	Access Control
260	Access Control Policy removed from disk: %s on VM: %s	H	true	Access Controls Policy removed.		Security	Access Control
261	New Access Control Policy: %s created.	L	false	New Access Control Policy Created.		Security	Access Control

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
262	Access Control Policy: %s updated. Policy now available as: %s.	H	false	Access Control Policy Updated.		Security	Access Control
263	Access Control Policy: %s deleted.	L	false	Access Control Policy Deleted.		Security	Access Control
264	Access Control Rule: %s added to Policy: %s.	H	false	New Access Control Rule added to Policy.		Security	Access Control
265	Access Control Rule: %s updated for Policy: %s.	H	false	Access Control Rule updated for Policy.		Security	Access Control
266	Access Control Rule: %s deleted from Policy: %s.	H	false	Access Control Rule deleted from Policy.		Security	Access Control
267	hytrust_accesscontrols rpm state changed to: %s on VM: %s	M	false	HyTrust Access Controls rpm state changed		Security	Access Control
268	Initiated application of Access Control Policy: %s to disk: %s on VM: %s.	H	false	Access Control Policy application initiated by Admin.		Security	Access Control
269	Initiated removal of Access Control Policy: %s from disk: %s on VM: %s.	H	false	Access Control Policy removal initiated by Admin.		Security	Access Control
270	Created Cloud VM Set %s with Single Encryption Key	L	true	CVMSet created with Single Encryption Key for dedup		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
271	Failed to upgrade KeyControl nodes: %s. Reverting upgraded nodes: %s.	L	true	Failed to upgrade KeyControl nodes.		Clusters	Upgrade
272	Failed to revert KeyControl nodes: %s. Remove nodes from KeyControl after reboot.	L	true	Failed to revert KeyControl nodes.		Clusters	Upgrade
273	Upgrade Cancelled. Error: %s	L	true	Failed to finalize upgrade.		Clusters	Upgrade
274	%s got reverted during upgrade. Reverting other nodes in the cluster to revision %s	L	false	Failed to upgrade KeyControl node.		Clusters	Upgrade
275	Successfully cancelled KeyControl Upgrade.	M	false	Cancelled KeyControl Upgrade.		Clusters	Upgrade
276	IP conflict detected for %ipaddr with MAC %this_mac on %this_month %this_day %this_time	H	true	Another VM is/ was using this KeyControl IP address.		Security	
277	Access Controls removed successfully on VM %s	H	true	Successful Access Controls removal on VM		Security	Access Control
278	Applying Policy %s, version %s failed on VM %s. %s	H	true	Policy application failure on VM with reason.		Security	Access Control
279	Applying Policy %s, version %s failed on disk %s of VM %s	H	true	Failure in Policy application on a specific disk of a VM.		Security	Access Control

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
280	Error removing Access Control Policy on disk %s of VM %s	H	true	Error removing Access Control Policy on a disk.		Security	Access Control
281	%s doesn't allow local user creation. Cannot support Access Controls	H	true	VM doesn't support Access Controls due to inability to create local users		Security	Access Control
282	%s doesn't allow ssh for localhost. Cannot support Access Controls	H	true	Cannot setup Access Controls on VM since it doesn't allow ssh for localhost		Security	Access Control
283	%s doesn't allow password-based ssh login. Cannot support Access Controls	H	true	Cannot setup Access Controls on VM since it doesn't allow password-based ssh login.		Security	Access Control
284	Access Control setup failed on VM %s. Please check /var/log/htac.log on VM for more details	H	true	Failure in initial Access Controls setup		Security	Access Control
285	Insufficient free space on %s to perform upgrade. Consult product documentation for procedure to add another disk	H	true	Disk does not have enough space for upgrade	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade
286	Access Control tampering detected on VM %s	H	true	Access Control Tampering		Security	Access Control

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
287	Error enforcing policy %s, version %s on VM %s. %s	H	true	Access Control Policy application failure due to htadmin error		Security	Access Control
288	New AD Server: %s created.	L	false	Create AD Server		Security	Active Directory
289	Updated AD Server config: %s.	L	false	Updated AD Server config		Security	Active Directory
290	Deleted AD Server: %s.	L	false	Deleted AD server		Security	Active Directory
291	User account htadmin already exists on VM %s. Please delete htadmin, before enforcing Access Control Policy	L	true	Local user account htadmin detected before Access Control pre-setup tests		Security	Access Control

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
292	VM - %s cannot verify communications from KeyControl because the KeyControl SSL certificate has changed but the CA certificate on the VM was not updated when the new SSL certificate was installed for KeyControl. To update the CA certificate on the VM and restore connectivity, log into the webGUI, download the latest CA certificate from Cloud tab > Actions > Download CA Certificate, copy the CA certificate to the VM, and execute "hcl update_ca -f pathtocert"	H	true	SSL certificate of KeyControl has changed and webserver has been restarted. One of the VMs did not receive the latest copy of the CA certificate to verify KeyControl. To restore communication, download the latest CA certificate from webgui cloud tab, copy it to the VM and execute hcl update_ca command		Security	Certificate
293	KMIP user certificate for %s has expired. KMIP client(s) that is/ are using the expired certificate will not be authenticated to perform KMIP operations. Please extend the user certificate or create new user certificate, and update the KMIP clients with the new certificate bundle	H	true	KMIP user certificate for one of the users has expired. KMIP client(s) using the expired certificate will not be authenticated to perform KMIP operations. Please create new KMIP certificate for the KMIP client(s) to use		Security	Certificate,KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
294	KMIP user certificate for %s will expire in %s days, %s hours and %s minutes. Upon expiry, client(s) that is/are using the expired certificate will not be authenticated to perform KMIP operations. Please extend the user certificate or create new user certificate, and update the KMIP clients with the new certificate bundle	H	true	KMIP user certificate for one of the users will expire soon. Upon expiry, KMIP client(s) using the expired certificate will not be authenticated to perform KMIP operations. Please create new KMIP certificate for the KMIP client(s) to use		Security	Certificate,KMIP
295	VM %s is using an older Hardware Signature format. Please run "hcl auth" cmd on the VM for a more secure signature.	H	true	VM is using an older Hardware Signature format. Please run "hcl auth" cmd on the VM for a more secure signature.		Security	Client
296		L	true	Alert email sent to Security Admins on upgrade.		Security	
297	Abandoning %d inactive tasks on %s. Abandoning %s task %s on %s not updated since %s, TaskId: %s	L	true	List of tasks that have been abandoned due to inactivity		Security	
298	Error!!! Could not enable support login. Please make sure there is enough space in the filesystem	H	true	Cannot enable support login. Please make sure there is enough space in the file-system	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	Support

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
299	Error!!! Could not disable support login. Please make sure there is enough space in the filesystem	H	true	Cannot disable support login. Please make sure there is enough space in the file-system	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	Support
300	%s attempting %s account login when object store is not readable	M	false	Attempt to login to support login in one of the KeyControl nodes when object store is down		Security	Support
301	Decryption is not allowed for device %s on VM %s. To decrypt: Access Control Policy : %s Version: %d must be removed from device. Auto Encryption Policy should be changed so as to exclude the device.	L	true	Device decryption refused due to applied policies.	Change policies as suggested in error message.	Security	
302	Space on HyTrust Bootloader partition %s is running low (%lld bytes free). Often times USN journal is the culprit. You can check USN journal size using the command: "fsutil usn queryjournal %s". To delete USN journal, use the command: "fsutil usn deletejournal /N %s "	H	true	Device decryption refused due to applied policies.	Change policies as suggested in error message.	Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
303	Login failure for %s from %s because %s is in lock out period.	M	false	Attempt to login to secroot in the lock out period after repeated unsuccessful login attempts		Security	Account
304	Changed AD group members for group %s. %s	L	false	List of AD Group members has been changed for a KeyControl Group		Security	Group
305	The current number of KeyControl nodes (%d) exceeds the maximum number of nodes allowed by your license (%d). You cannot add any more KeyControl nodes to this cluster until you upgrade your license.	M	true	KeyControl nodes in use exceeds license limit of installed license		Security	Licensing
306	The current number of VMs registered with this KeyControl cluster (%d) exceeds the maximum number of VMs allowed by your license (%d). You cannot register any additional VMs until you upgrade your license.	M	true	Registered VM count exceeds license limit of installed license		Security	Licensing
307	Service %s is up	L	false	KeyControl system service is up		Security	System Service
308	Service %s is down	H	true	KeyControl system service is down		Security	System Service

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
309	Using AD group membership for %s - %s	M	false	ADgroup membership of the AD user that was returned by the LDAP server during first time login. The ADgroup membership will be used to determine the KeyControl Group membership of the AD user.		Security	Licensing
310	Updating AD group membership for %s - %s	M	false	ADgroup membership of the AD user that was returned by the LDAP server. The new ADgroup membership will be used to determine the KeyControl Group membership of the AD user who has already logged into KeyControl previously.		Security	Licensing
311	Added KMIP client configuration. Server: %s	L	false	Added KMIP client configuration		Security	KMIP Client
312	Updated KMIP client configuration. Server: %s	L	false	Updated KMIP client configuration		Security	KMIP Client
313	Deleted KMIP client configuration. Server: %s	H	true	Deleted KMIP client configuration		Security	KMIP Client

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
314	Deleted all KMIP client configurations.	H	true	Deleted KMIP client configuration		Security	KMIP Client
315	Failed to delete key:%s on external KMIP server	M	false	Failed to delete key on KMIP server		Security	KMIP Client
316	Added AD Domain: %s	L	false	Added a new AD Domain		Security	LDAP
317	Updated AD Domain %s. Changed Attributes - %s	L	false	Updated the AD Domain		Security	LDAP
318	Remomved AD Domain %s	L	false	Removed AD Domain from KeyControl		Security	LDAP
319	Added new Domain Controller %s for AD Domain %s	L	false	Added a new AD Domain Controller		Security	LDAP
320	Updated Domain Controller %s for AD Domain %s. Changed Attributes - %s	L	false	Updated Domain Controller		Security	LDAP
321	Removed Domain Controller %s for AD Domain %s	L	false	Removed Domain Controller from KeyControl		Security	LDAP
322	encrypt failed for device %s on VM %s, error %d	M	true	Encrypt operation failed on VM		Security	Client
323	decrypt failed for device %s on VM %s, error %d	M	true	Decrypt operation failed on VM		Security	Client

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
324	rekey failed for device %s on VM %s, error %d	M	true	Rekey operation failed on VM		Security	Client
325	Successfully deleted admin key on EKS: %s	M	false	Successfully deleted admin key on KMIP server		Security	KMIP Client
326	Successfully generated admin key on EKS: %s	M	false	Successfully generated admin key on KMIP server		Security	KMIP Client
327	Failed to generate admin key on EKS: %s	H	true	Failed to generate admin key on KMIP server		Security	KMIP Client
328	Failed to store admin key on EKS: %s	H	true	Failed to store admin key on KMIP server		Security	KMIP Client
329	Successfully stored admin key on EKS: %s	M	false	Successfully stored admin key on KMIP server		Security	KMIP Client
330	Failed to fetch admin key from EKS: %s	M	true	Failed to fetch admin key from KMIP server		Security	KMIP Client
331	KeyControl Upgrade failed. Please contact Support	H	true	Post upgrade failed		Clusters	Rolling Upgrade
332	Domain Controllers re-ordered for %s	L	false	Order of Domain Controllers has been changed for an AD domain configured		Security	LDAP
333	Failed to set backup hosts to %s on %s	H	true	Failed to update backup hosts		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
334	Virtual Machine %s is in BoundaryControl grace period	M	true	VM in Boundary Control grace period		Security	Boundary Control
335	Virtual Machine %s, BoundaryControl grace period expired	M	true	VM Boundary Control grace period expired		Security	Boundary Control
336	Application Link created from Product (%s) Version (%s) IP List (%s)	L	false	A new Application Link has been created from an external product. This link will allow the external product to make API calls to KeyControl.		Clusters	AppLink
337	Application Link renewed for Product (%s) Version (%s) IP List (%s)	L	false	An Application Link has been renewed for the external product.		Clusters	AppLink
338	Failed to upgrade LDAP Settings. Please reconfigure LDAP settings manually	H	true	Failed to upgrade LDAP Settings.		Security	LDAP
339	Failed to store adminkey on HSM	H	true	Failed to store adminkey on HSM		Security	HSM
340	Removed Server(s) %s from Domain %s	L	true			Clusters	
341	Grace period will expire on %s for Virtual Machine %s, please check connectivity	H	true			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
342	Grace period expired for Virtual Machine %s, please authenticate again	H	true			Security	
343	Virtual Machine %s, failed to update following attributes: %s	H	false	Failed to update Virtual Machine settings		Security	
344	Finished propagating changed attributes: %s to all Virtual Machines in Cloud VMSet: %s	H	false	Propagation of changed attributes completed for CVMSet		Security	
345	Invalid software was discovered on KeyControl system %s. This is a possible trojan horse attack. Contact Support for assistance	H	true	Whitelisting violation detected on production build		Security	Whitelisting
346	Entrust Whitelist validation on KeyControl system %s has discovered modified files. These changes are allowed for development systems, but please review Whitelist logs for correctness.	L	true	Whitelisting violation detected on development build		Security	Whitelisting
347	Could not set password for %s: %s	H	true	Failed to set password		Security	
348	Password changed for %s	H	true	Password changed		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
349	Enabled %s user	H	true	Enabled user		Security	
350	Failed to enable %s user	H	true	Failure in enabling user		Security	
351	Disabled %s account	H	true	Disable account		Security	
352	%s user logged out successfully	L	false	User logout		Security	
353	Could not download the certificate: %s	M	true	Download certificate failure		Security	
354	Downloaded a new CA certificate	M	true	Downloaded CA certificate		Security	
355	ssh %sd for %s	M	false	SSH enabled/ disabled for user		Security	
356	Failed to %s ssh for %s	M	false	Failure in enabling/disabling SSH for user		Security	
357	KeyControl restored from version %s backup file	M	false	KeyControl restored from backup successfully		Security	
358	License auto-update: %s	M	true	License change during auto-update		Security	
359	Failed to %s syslog on %s	H	true	Failed to enable/ disable syslog on KeyControl node(s)		Security	syslog

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
360	Generated Syslog Certificate Signing Request with common name %s	L	false	Generated Syslog Certificate Signing Request with common name		Security	syslog
361	Changed following Syslog settings attributes: %s	L	false	Changed some Syslog settings attributes.		Security	syslog
362	Exporting audit log succeeded for %s (%s). Audit log is available to download.	M	true	Finish exporting audit log		Security	
363	Exporting audit log failed for %s (%s).	M	true	Exporting audit log failed		Security	
364	CVM Certificate %s, associated with CVM %s, CVMSet %s, revoked successfully	H	true			Security	Certificate
365	Cloud VM Set creation failed. Error: Failed to create root key in HSM. %s.	H	true	Root key creation failure on HSM during Cloud VM Set creation.	Security Admin should determine whether HSM is properly configured.	Security	Key Encryption Key
366	Cloud VM Set creation failed. Error: Failed to generate wrapped Key Encryption Key in HSM. %s.	H	true	Wrapped Key Encryption Key generation failed on HSM during Cloud VM Set creation	Security Admin should determine whether HSM is properly configured..	Security	Key Encryption Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
367	Virtual Machine %s moved from Cloud VM Set - %s (in KeyControl Group - %s) to Cloud VM Set - %s in (KeyControl Group - %s)	M	true	Virtual Machine has been moved from Cloud VM Set to another one (might be in another KeyControl Group		Security	
368	Successfully enabled passphrase based startup authentication	M	false	Set startup authentication type		Clusters	Startup Authentication
369	Successfully changed passphrase for startup authentication	M	false	Changed passphrase for startup authentication		Clusters	Startup Authentication
370	Recovered access to KeyControl node %s using passphrase	M	true	Recovered Masterkey using passphrase		Clusters	Startup Authentication
371	Successfully disabled passphrase based startup authentication	M	false	Set startup authentication type		Clusters	Startup Authentication
372	Successfully reset nShield HSM configuration	M	false	nShield HSM configuration reset		Security	HSM
373	Cloud VM Set %s: Asymmetric KeyID %s created.	M	false	Asymmetric KeyID created		Security	Asymmetric KeyID
374	Cloud VM Set %s: Asymmetric KeyID %s revoked/unrevoked.	M	false	Asymmetric KeyID revoked/ unrevoked		Security	Asymmetric KeyID
375	Cloud VM Set %s: Asymmetric KeyID %s updated - expires %s, onexpiry %s.	M	false	Asymmetric KeyID expiration attributes updated		Security	Asymmetric KeyID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
376	Cloud VM Set %s: Asymmetric KeyID %s description updated.	M	false	Asymmetric KeyID description updated		Security	Asymmetric KeyID
377	Cloud VM Set %s: Asymmetric KeyID %s deleted.	M	false	Asymmetric KeyID deleted		Security	Asymmetric KeyID
378	Successfully encrypted plaintext using KeyID: %s	M	false	Encrypted plaintext using keyid key		Security	KeyID
379	Successfully decrypted ciphertext using KeyID: %s	M	false	Decrypted ciphertext using keyid key		Security	KeyID
380	Cloud VM Set %s: Asymmetric KeyID %s has expired	M	true	Asymmetric KeyID expired		Security	Asymmetric KeyID
381	Fatal error on KeyControl nodes: %s. Please contact Support	H	true	KeyControl Upgrade Failure	Reinstall specified nodes to secure KeyControl Cluster	Security	Rolling Upgrade
382	CRL regenerated and applied successfully on %s	M	false	CRL regeneration		Security	Certificate
383	Attempt to register a new KeyControl node (%s) with revision %s failed. Error: %s	M	true	Attempt to register a new KeyControl node failed		Clusters	Cluster Node Join
384	Successfully reset %s	M	true	The KeyControl node has been reset.		Clusters	Cluster Node Join

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
385	%s. Please contact HyTrust to buy/renew the license. If you do not plan to use this feature, you should delete your existing vault(s) to stop this message. For more information, see the Administration Guide.	M	true	Vault license not enabled or expired		Security	Licensing
386	Created Secrets Vault %s	M	false	The specified vault has just been created.		Security	Secrets Vault
387	Successfully removed pre-upgrade snapshots.	M	true	KC pre-upgrade snapshots were removed.		Clusters	Upgrade
388	KeyControl node {$myip[0]}/ {$myhost[0]} removed pre-upgrade snapshots.	M	true	KC pre-upgrade snapshots were removed from a node.		Clusters	Upgrade
389	KeyControl configuration has been successfully updated. New node %s needs to be added to nShield HSM server configuration	M	true	Update nShield HSM server configuration		Security	HSM
390	Failed to configure newly joined node %s for nShield HSM server	H	true	Failed to configure node for nShield HSM		Security	HSM
391	Successfully completed decryption of KMIP objects	H	true	Decrypt operation completed for KMIP objects		Security	KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
392	Successfully completed rekey of KMIP objects	H	true	Rekey operation completed for KMIP objects		Security	KMIP
393	Successfully enabled encryption of KMIP objects	H	true	Enabled encryption of KMIP objects		Security	KMIP
394	Successfully disabled encryption of KMIP objects	H	true	Disabled encryption of KMIP objects		Security	KMIP
395	Failed to generate Key Encryption Key on HSM. Error: %s	H	true	Failed to generate Key Encryption Key on HSM		Security	KMIP
396	Successfully generated Key Encrytion Key on HSM	M	false	Generated Key Encryption Key on HSM		Security	KMIP
397	Successfully cancelled node-join	M	false	Cancelled KeyControl Node-Join		Clusters	Cluster Node Join
398	Failed to join %s to KeyControl Cluster. Error: %s	M	true	Failed to join KeyControl node		Clusters	Cluster Node Join
399	Successfully joined %s to KeyControl Cluster	M	false	Added new node to KeyControl Cluster		Clusters	Cluster Node Join
400	CSR generated with common-name %s for node-join	M	false	Certificate Signing Request generated for node-join		Clusters	Cluster Node Join
401	Certificate bundle generated for node-join	M	false	Certificate bundle generated for node-join		Clusters	Cluster Node Join

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
402	Returning keys to VM %s running on ESXi Host %s. VM UUID is %s.	M	false	Returning keys to VM on successful authorization with HTCC with additional VM info		Security	GET-KEY Container
403	Returning keys to VM %s	M	false	Returning keys to VM on successful authorization with HTCC		Security	GET-KEY Container
404	NTP servers not found on KeyControl %s	H	true	NTP servers not found on KeyControl	Configure NTP servers using KeyControl TUI	Clusters	NTP
405	NTP synchronization failed on KeyControl %s	M	true	NTP synchronization failed on KeyControl	Check if NTP servers are reachable from KeyControl	Clusters	NTP
406	Freespace available on %s has fallen below %s%% for the /boot volume. Please contact support.	H		The amount of free disk space on the KeyControl appliance /boot filesystem has dropped below our recommended threshold. Please contact support for assistance.	Contact support.	Clusters	
407	Set Key Encryption Key expiry to %s, onexpiry to %s for Cloud VMSet %s. Initiated rekey process to encrypt all Data Encryption Keys.	M	false	Added Key Encryption Key to Cloud VMSet		Security	Key Encryption Key

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
408	Successfully encrypted Data Encryption Keys of all CVMs in CVMSet: %s with a Key Encryption Key: %s. %s VMs, %s KeyIDs %s Asymmetric KeyIDs affected	M	false	Successfully encrypted Data Encryption Keys with Key Encryption Key		Security	Key Encryption Key
409	Successfully reset Luna HSM configuration	M	false	Luna HSM configuration reset		Security	HSM
410	Successfully tested nShield HSM configuration	M	false	nShield HSM configuration was successfully tested		Security	HSM
411	Luna HSM configuration changed:-	M	false	Luna HSM configuration changed		Security	HSM
412	Successfully tested Luna HSM configuration	M	false	Luna HSM configuration was successfully tested		Security	HSM
413	Luna Cloud HSM configuration changed:-	M	false	Luna Cloud HSM configuration changed		Security	HSM
414	Successfully reset Luna Cloud HSM configuration	M	false	Luna Cloud HSM configuration was reset		Security	HSM
415	Successfully tested Luna Cloud HSM configuration	M	false	Luna Cloud HSM configuration was successfully tested		Security	HSM

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
416	Failed to create / bootext filesystem. Please contact support for more assistance	H	true	Failed to create / bootext filesystem. Please contact support for more assistance		Security	
417	Failed to join %s/%s to KeyControl Cluster. Please contact Support	H	true	Failed to join KeyControl node to cluster		Clusters	Cluster Node Join
418	CloudKey: {} in KeySet {} modified	M	true	CloudKey: {} in KeySet {} modified		Security	BYOK
419	CloudKey: {} in KeySet {} migrated to HSM	M	false	CloudKey: {} in KeySet {} migrated to HSM		Security	BYOK
420	Cloud Key {} deleted from KMS	H	true	Cloud Key {} deleted from KMS		Security	BYOK
421	Cloud Key {} restored to KMS	M	true	Cloud Key {} restored to KMS		Security	BYOK
422	Cloud Key {} state changed to {} on KMS	H	true	Cloud Key {} state changed to {} on KMS		Security	BYOK
423	Tag {} (value {}) set on Cloud Key {}	M	false	Tag {} (value {}) set on Cloud Key {}		Security	BYOK
424	Removed Tag {} on Cloud Key {}	M	false	Removed Tag {} on Cloud Key {}		Security	BYOK
425	Set users ({}) and administrators ({}) to Cloud Key {}	M	true	Set users ({}) and administrators ({}) to Cloud Key {}		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
426	Removed {} ({}) from Cloud Key {}	M	true	Removed {} ({}) from Cloud Key {}		Security	BYOK
427	New Cloud Key {} created in KeySet {}	M	true	New Cloud Key {} created in KeySet {}		Security	BYOK
428	New Cloud Key {} created in KeySet {} {} {}	M	true	New Cloud Key {} created in KeySet {} Region/Vault {}		Security	BYOK
429	Cloud Key {} in KeySet {} uploaded to {} {}	M	true	Cloud Key {} in KeySet {} uploaded to {} {}		Security	BYOK
430	Cloud Key {} in KeySet {} rotated	M	true	Cloud Key {} in KeySet {} rotated		Security	BYOK
431	Cloud Key {} in KeySet {} scheduled for deletion in {} days	H	true	Cloud Key {} in KeySet {} scheduled for deletion in {} days		Security	BYOK
432	Deletion schedule canceled on Cloud Key {} in KeySet {}	M	true	Deletion schedule canceled on Cloud Key {} in KeySet {}		Security	BYOK
433	Cloud Key {} in KeySet {} deletion complete	M	false	Cloud Key {} in KeySet {} deletion complete		Security	BYOK
434	Processed Expiry Action {} on Cloud Key {} in KeySet {}	H	true	Processed Expiry Action {} on Cloud Key {} in KeySet {}		Security	BYOK
435	Cloud Key {} region {} imported in KeySet {}	M	false	Cloud Key {} region {} imported in KeySet {}		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
436	Started Key Import from {} {} from KMS to KeySet {}	M	true	Started Key Import from region/keyvault/keyring {} from KMS to KeySet {}		Security	BYOK
437	Keys imported from {} {} from KMS to KeySet {}	M	true	Keys imported from region/keyvault/keyring {} from KMS to KeySet {}		Security	BYOK
438	Keys imported from AWS KMS to KeySet {}	M	true	Keys imported from AWS KMS to KeySet {}		Security	BYOK
439	Keys migrated to HSM from KEYCONTROL for KeySet {}	H	true	Keys migrated to HSM from KEYCONTROL for KeySet {}		Security	BYOK
440	KeySet: {} modified	M	true	KeySet: {} modified		Security	BYOK
441	Started key migration, from KEYCONTROL to HSM, for KeySet {}	H	true	Started key migration, from KEYCONTROL to HSM, for KeySet {}		Security	BYOK
442	New KeySet: {} created	M	true	New KeySet: {} created		Security	BYOK
443	Key Set {} deleted	H	true	Key Set {} deleted		Security	BYOK
444	CSP Account: {} modified	M	true	CSP Account: {} modified		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
445	CSP Account {} access keys rotated	H	true	CSP Account {} access keys rotated		Security	BYOK
446	New CSP Account: {} created	M	true	New CSP Account: {} created		Security	BYOK
447	CSP Account {} deleted	H	true	CSP Account {} deleted		Security	BYOK
448	Access key rotation failed	H	true	Access key rotation failed		Security	BYOK
449	CloudKey rotation failed	M	true	CloudKey rotation failed		Security	BYOK
450	CloudKey expiry processing failed	M	true	CloudKey expiry processing failed		Security	BYOK
451	CloudKey import failed	M	true	CloudKey import failed		Security	BYOK
452	CloudKey auto import failed	M	true	CloudKey auto import failed		Security	BYOK
453	Set Key Policy for Cloud Key {}	M	true	Set Key Policy for Cloud Key		Security	BYOK
454			false			Security	Upgrade
455	Encryption finished on system volumes of KeyControl {}	M	false	Encryption finished on system volumes of KeyControl		Clusters	BYOK
456	Successfully installed managed Secret Vault Plugin: {} (version {})	M	false	Managed Secret Vault Plugin install success		Security	Secrets Vault

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
457	Cloud Key {} in KeySet {} deleted as upload failed	L	false	Cloud Key object deleted as upload failed		Security	BYOK
458	Enabled Root-of-Trust in password mode	M	false	Enabled Root-of-Trust in password mode		Security	HSMROT
459	Failed to enable Root-of-Trust	M	false	Failed to enable Root-of-Trust		Security	HSMROT
460	Enabled Root-of-Trust in hwsig mode	M	false	Enabled Root-of-Trust in hwsig mode		Security	HSMROT
461	Failed to enable Root-of-Trust	M	false	Failed to enable Root-of-Trust		Security	HSMROT
462	Disabled Root-of-Trust	M	false	Disabled Root-of-Trust		Security	HSMROT
463	Failed to disable Root-of-Trust: %s	M	false	Failed to disable Root-of-Trust: %s		Security	HSMROT
464	A differenet Cloud Key with name {} for KeyVault {} is already present in KeySet {}.If you want to overwrite the key in Key Control, delete the existing key from key control and import again	M	true	Could not import cloudkey as a different key with the same keyname already present in Key Control		Security	BYOK
465	Created new KMIP tenant {} with Active Directory domain {} and Active Directory user/group {} as initial KMIP administrator	M	true	Created new KMIP tenant with its own Active Directory config and an Active Directory user/group for initial access		Security	KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
466	Deleted KMIP tenant {}	M	true	Deleted KMIP tenant		Security	KMIP
467	Internal web server certificate of %s has expired. A new certificate must be installed for KeyControl Cluster to be healthy	H	true	Certificate used by the internal web server of one of the nodes has expired. Domain administrator has to install a new certificate for the KeyControl cluster to be healthy.		Clusters	Certificate
468	Internal web server certificate of %s will expire in %s days, %s hours and %s minutes. A new certificate must be installed before the current one expires for the KeyControl Cluster to be healthy.	H	true	Certificate used by the internal web server of one of the nodes is about to get expired. Domain administrator has to install a new certificate before it gets expired. Otherwise cluster will be degraded		Clusters	Certificate
469	Cloud Key {} KeyVault {} in KeySet {} synced from KMS	M	false	Cloud Key {} KeyVault {} in KeySet {} synced from KMS		Security	BYOK
470	Cloud Key {} operations changed to {} on Azure KMS	M	true	Cloud Key {} operations changed to {} on Azure KMS		Security	BYOK
471	Cloud Key {} KeyVault {} imported in KeySet {}	M	false	Cloud Key {} KeyVault {} imported in KeySet {}		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
472	CloudKey import failed in KeyVault {} KeySet {} Error {}	M	false	CloudKey import failed in KeyVault {} KeySet {} Error {}		Security	BYOK
473	Client Secret for Service application {} (CSP {}) will expire on {}. Please update it now to avoid BYOK management service disruption	H	true			Security	
474	Client Secret for Service application {} (CSP {}) has expired on {}. Please update it now to resume BYOK management service	H	true			Security	
475	Successfully started migration of KMIP objects to multi-tenant KMIP server	M	false	Started migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
476	Successfully completed migration of KMIP objects to multi-tenant KMIP server	M	false	Completed migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
477	Successfully cancelled migration of KMIP objects to multi-tenant KMIP server	M	false	Cancelled migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
478	Successfully sent KMIP tenant account verification email to %s	M	false	Sent KMIP tenant account verification email		Security	KMIP

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
479	Successfully reset administrator account password of KMIP vault %s	M	false	Reset KMIP vault administrator account password		Security	KMIP
480	Successfully reset administrator account password of Secrets vault %s	M	false	Reset Secrets vault administrator account password		Security	Secrets Vault
481	Failed to initialize Authentication database	M	true			Security	oidc
482	Cloud Key {} KeyRing {} imported in KeySet {}	M	false	Cloud Key {} KeyRing {} imported in KeySet {}		Security	BYOK
483	Cloud Key {} KeyRing {} in KeySet {} synced from KMS	M	false	Cloud Key {} KeyRing {} in KeySet {} synced from KMS		Security	BYOK
484	CloudKey import failed in KeyRing {} KeySet {} Error {}	M	false	CloudKey import failed in KeyRing {} KeySet {} Error {}		Security	BYOK
485	Label {} (value {}) set on Cloud Key {}	M	false	Label {} (value {}) set on Cloud Key {}		Security	BYOK
486	Removed Label {} on Cloud Key {}	M	false	Removed Label {} on Cloud Key {}		Security	BYOK
487	Failed to delete old access keys for CSP Account '{}'. Error - '{}'	M	false	Failed to delete old access keys for CSP Account '{}'. Error - '{}'		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
488	EKM Key Access Justification policy violation while accessing Cloud Key {} in KeySet {} : error {}	M	false	EKM Key Access Justification policy violation		Security	BYOK
489	TDE Connector {} state changed to {} on Keyset {}	M	true	TDE Connector state changed		Security	BYOK
490	TDE Connector {} expiry date changed to {} on Keyset {}	M	true	TDE Connector expiry date changed		Security	BYOK
491	Added TDE Connector {} for CVM {} in KeySet {}	M	true	Add TDE connector		Security	BYOK
492	Removed TDE Connector {} from CVM {} in KeySet {}	M	true	Remove TDE connector		Security	BYOK
493	Successfully registered with KCM (KeyControl Compliance Manager) (id: {}) from {}	M	true	KCM (KeyControl Compliance Manager) register		Security	KCM
494	Successfully unregistered with KCM (KeyControl Compliance Manager) (id: {}) from {}	M	true	KCM (KeyControl Compliance Manager) unregister		Security	KCM
495	Successfully reset KCM (KeyControl Compliance Manager) registration configuration from {}	M	true	KCM (KeyControl Compliance Manager) configuration reset		Security	KCM
496	User %s reset syslog settings	M	false	Reset Syslog settings		Security	syslog

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
497	Attempt to register a new node, named server "%s" failed -- maximum node limit reached.	M	true	Maximum allowed cluster node count reached		Security	Licensing
498	Backup failed due to insufficent space on root device. Please contact support.	H	true	Backup failed due to insufficent space on root device		Security	Backup
499	Backup was not started due to heavy load on %s	M	true	Backup was not started due to heavy load on KeyControl		Security	Backup
500	'%s can be downloaded from the Settings page (https://%s/appliance/#!/account). Reason for regeneration: %s	H	true	Regenerated Admin Key		Security	Appliance
501	Rescued %s vault: %s	L	true	Rescued Vault		Security	Account
502	%s logged in from ipaddr %s using Personal Access Token %s	L	false	The specified user has just logged in from the IP address shown with Personal Access Token.		Security	Personal Access Token
503	AD authorization(Personal Access Token login) for user %s failed. Reason :- %s		false	Reason for AD/LDAP login failure for Personal Access Token login		Security	Personal Access Token

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
504	%s %s Personal Access Token %s from ipaddr %s		false	Create/Update/Delete Actions on Personal Access Token		Security	Personal Access Token
505	Keys migrated from HSM to KEYCONTROL for KeySet {}	H	true	Keys migrated from HSM to KEYCONTROL for KeySet {}		Security	BYOK
506	CloudKey: {} in KeySet {} migrated to KEYCONTROL	M	false	CloudKey: {} in KeySet {} migrated to KEYCONTROL		Security	BYOK
507	Keys migrated from KEYCONTROL to HSM for KeySet {}	H	true	Keys migrated from KEYCONTROL to HSM for KeySet {}		Security	BYOK
508	Updated %s Vault %s with KCM %s	M	false	The specified vault has just been updated with KCM.		Security	KCM
509	Configured OIDC without AD with client id %s	M	false	Configured OIDC without AD		Security	AUTHENTICATION
510	OIDC without AD configuration removed	M	false	OIDC without AD configuration removed		Security	AUTHENTICATION
511	Changed Password Settings :- %s from %s to %s	M	false	One or more of the listed password settings has been changed.		Security	Configuration

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
512	Keys cached from HSM to KEYCONTROL for KeySet {}	H	true	Keys cached from HSM to KEYCONTROL for KeySet {}		Security	BYOK
513	Keys uncached from KEYCONTROL for KeySet {}	H	true	Keys uncached from KEYCONTROL for KeySet {}		Security	BYOK
514	CloudKey: {} in KeySet {} cached to KeyControl	M	false	CloudKey: {} in KeySet {} cached to KeyControl		Security	BYOK
515	CloudKey: {} in KeySet {} uncached from KeyControl	M	false	CloudKey: {} in KeySet {} uncached from KeyControl		Security	BYOK
516	OIDC authorization failed. Reason :- %s	M	false	Reason for OIDC login failure		Security	AUTHENTICATION
517	Connection from node %s to HSM %s has failed	H	true	The node is unable to communicate with the HSM	Security Admin should check the HSM configuration.	Security	HSM
518	Connection from node %s to HSM %s is restored	L	true	The node is able to communiucate with the HSM again		Security	HSM
519	Connection from node %s to HSM %s still failed after HSMROT timeout, locking down	H	true	The node is shutting down because it has lost contact with the HSM	Fix the issue preventing the node from contacting the HSM and restart the node.	Security	HSM

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
520	HSM issue on node %s: %s	M	true	Some HSM issues have been detected on the node that do not prevent communication with the HSM	Security Admin should check the HSM configuration.	Security	HSM
521	HSM issues resolved on node %s	L	true	The HSM issues previously reported on the node have been resolved		Security	HSM
522	Failed to install self-signed certificate cluster-wide	M	true	Install self signed certificate cluster-wide		Clusters	
523	Failed to clean cacert list.	M	false	Clean cacert list guid from system setting		Clusters	
524	Successfully moved the cluster to self-signed certificate.	M	false	Install self signed certificate cluster-wide		Clusters	
525	Successfully changed the EMS Enforcement crypto policy.	M	false	Change EMS Enforced Configuration		Clusters	
526	The license for this system expired %s days ago. Please renew or upgrade the license. Start that process from the licensing page in the webgui at https://%s/appliance/#!/license	H	true	License expired		Security	Licensing

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
527	The license for this system expires in %s days. Please renew or upgrade the license. Start that process from the licensing page in the webgui at https://%s/appliance/#!/license	H	true	License will expire after some days.		Security	Licensing
528	The license for this system expires today. Please renew or upgrade the license. Start that process from the licensing page in the webgui at https://%s/appliance/#!/license	H	true	License is expiring today.		Security	Licensing
529	This system has exceeded the licensed limit of %s Virtual Machines. Further Virtual Machine creation is disabled. Please renew or upgrade the license. Start that process from the licensing page in the webgui at https://%s/appliance/#!/license	H	true	This system has exceeded the licensed limit of virtual machines count. Further Virtual Machine creation is disabled.		Security	Licensing
530	This system has exceeded the licensed limit of %s Virtual Machines. Please renew or upgrade the license. Start that process from the licensing page in the webgui at https://%s/appliance/#!/license	H	true	This system has exceeded the licensed limit of virtual machines count.		Security	Licensing

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
531	System Initialization Complete	L	false	System Initialization Complete		Security	
532	System Autoconfiguration Complete	L	false	System Autoconfiguration Complete		Security	
533	Cloud Key {} in KeySet {} replicated to {}	M	true	Cloud Key {} in KeySet {} replicated to {}		Security	BYOK
534	The Cloud Key {} from KeySet {} will be rotated on {}.	H	true	Send notification before cloudkey rotation.		Security	BYOK
535	The Cloud Key {} from KeySet {} is expiring on {} with the Action {}.	H	true	Send notification before cloudkey expiration.		Security	BYOK
536	System has completed automatic renewal of self-signed certificates.	L	false	Automatic renewal of self-signed certificates.		Clusters	
537	System has completed automatic renewal of CA certificates.	L	false	Automatic renewal of CA certificates.		Clusters	
538	Probable LOW DISK SPACE: refreshing KMIP database is failing. Most probably the disk is low on space. Please consider increasing disk space.	H	true			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
539	Generated Access Token for TDE Connector {} in KeySet {}	M	true	Add TDE connector		Security	BYOK
540	Internal CA signed certificate with common name and SANs - '%s', '%s' is generated and installed.	L	false	New internal CA signed certificate generated and installed.		Clusters	Certificate
541	KeyControl upgrade failed. Failed to revert nodes. Please contact Support	H	true	Post upgrade failed		Clusters	Rolling Upgrade
542	Failure to change the EMS Enforcement crypto policy. Reverting to %s	M	false	Change EMS Enforced Configuration		Clusters	
543	NTP synchronization succeeded on KeyControl %s	M	true	NTP synchronization succeeded on KeyControl	Check if NTP servers are reachable from KeyControl	Clusters	NTP
544	Backup of Cloud Key {} failed: {}	M	true	Backup of Cloud Key {} failed: {}		Security	BYOK
545	Cloud Key {} backup {} is not available in remote storage	M	true	Cloud Key {} backup {} is not available in remote storage		Security	BYOK
546	Unsupported ciphers found in KMIP server configuration: %s	L	true	Unsupported ciphers found in KMIP server configuration		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
547	Updated default cipher list to %s in KMIP server configuration	L	true	Updated default cipher list to %s in KMIP server configuration		Security	
548	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled deletion has been cancelled	M	true	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled deletion has been cancelled		Security	BYOK
549	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled expiry has been cancelled	M	true	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled expiry has been cancelled		Security	BYOK
550	CSP Account: {} access credentials are due rotation. Please rotate through the Salesforce UI.	M	true	CSP Account: {} access credentials are due rotation.		Security	BYOK
551	Started HSM key caching for KeySet {}	M	true	Started HSM key caching for KeySet {}		Security	TDE
552	Keys cached to HSM for KeySet {}	M	true	Keys cached to HSM for KeySet {}		Security	TDE

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
553	CSP Account {} failed to access AWS global infra API with the default region. The key management capabilty is unaffected, but some region's full names may not be displayed.	L	true	Unable to access AWS global infra API		Security	BYOK
554	Certificate based authentication enabled on CSP Account {}	M	true	Certificate based authentication enabled on CSP Account {}		Security	BYOK
555	Certificate based authentication disabled on CSP Account {}	M	true	Certificate based authentication disabled on CSP Account {}		Security	BYOK
556	Failed to create new client secret for CSP Account {}. Error {}	M	true	Failed to create new client secret for CSP Account {}. Error {}		Security	BYOK
557	CloudKey {} status changed from {} to {} on synchronization with Cloud	M	true	CloudKey {} status changed from {} to {} on synchronization with Cloud"		Security	BYOK
558	Cache only key replay attack detected on csp {}	H	true	Cache only key replay attack detected		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
559	"To comply with certificate validity of KCV's CA signed server certificate, we will auto renew it on %s for %s. If you have VME-vault, please ensure the re-authentication of all VMs after that renewal.	H	true	"To comply with certificate validity of KCV's CA signed server certificate, we will auto renew it on %s for %s. If you have VME-vault, please ensure the re-authentication of all VMs after that renewal.		Security	Certificate
560	CloudKey {} KeySet {} cannot be migrated to FIPS level 3 HSM because it uses cipher {}.	M	false	CloudKey {} KeySet {} cannot be migrated to FIPS level 3 HSM because it uses cipher {}.		Security	BYOK
561	Unknown error in check_ncipher_data - %s	H	true	Unknown error in HSM files		Security	HSM
562	Failed to clear error in check_ncipher_data - %s	H	true	Failed to clear error in HSM files		Security	HSM
563	KCV has renewed the CA certificate that is being used by KCV's external web server.	M	false	KCV has renewed the CA certificate that is being used by KCV's external web server.		Security	Certificate
564	KCV has renewed the CA certificate that is being used by KCV's internal web server.	M	false	KCV has renewed the CA certificate that is being used by KCV's internal web server.		Security	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
565	KCV's internal CA certificate, used for external communication (external webserver) will expire on %s. KCV will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. We recommend to re-authenticate all vms connected to VME-vault using the commands 'hcl updatecert -a' and 'hcl auth -a' after the renewal. If your vault uses client certificate, then please generate new client certificate and use it at client application after the renewal.	M	true	KCV's internal CA certificate, used for external communication (external webserver) will expire on %s. KCV will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. We recommend to re-authenticate all vms connected to VME-vault using the commands 'hcl updatecert -a' and 'hcl auth -a' after the renewal. If your vault uses client certificate, then please generate new client certificate and use it at client application after the renewal.		Security	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
566	KCV's internal CA certificate, used for internal communication (internal webserver) will expire on %s. KCV will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. If your cluster is in a degraded state following the renewal, reboot each node individually, making sure to reboot the master node last.	M	true	KCV's internal CA certificate, used for internal communication (internal webserver) will expire on %s. KCV will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. If your cluster is in a degraded state following the renewal, reboot each node individually, making sure to reboot the master node last.		Security	Certificate
567	OIDC CA Certificate Uploaded Successfully	M	false	OIDC CA Certificate Uploaded Successfully		Security	OIDC
568	{} purged KeyVault {}.	M	true	{} purged KeyVault {}.		Security	BYOK
569	KC self-signed certificate for {server.hostname} (use for external webserver) is renewed.	L	false	KC self-signed certificate for {server.hostname} (use for external webserver) is renewed.		Security	Certificate

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
570	KC self-signed certificate for {server.hostname} (use for internal webserver) is renewed.	L	false	KC self-signed certificate for {server.hostname} (use for internal webserver) is renewed.		Security	Certificate
571	Failed to migrate Azure Keyvaults to target keyset {}. Error: {}.	M	true	Failed to migrate Azure Keyvaults to target keyset {}. Error: {}.		Security	BYOK
572	{} started migration of Azure keyvaults from source KeySets {} to target KeySet {}	M	true	Azure Keyvault migration between KeySets started		Security	BYOK
573	Migration of Azure Keyvaults to {} did not complete successfully. Expected {} cloud keys and {} key versionss but found {} cloud keys and {} key versions.	M	true	Azure Keyvault migration between KeySets partially completed		Security	BYOK
574	Migration of Azure Keyvaults to {} completed successfully	M	true	Azure Keyvault migration between KeySets completed		Security	BYOK
575	Warning: CSP Account {} manages keys in overlapping subscriptions with existing Azure CSP accounts: {}. Subscription IDs: {}	M	true	Azure CSP created with overlapping subscriptions with existing Azure CSP accounts		Security	BYOK
576	Could not process {} on AWS Cloud Key {}. {}. The key has been disabled instead.	M	true	AWS Cloudkey expiry action failed.		Security	BYOK

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
577	Changed AD group members for group Appliance. %s	L	false	List of AD Group members has been changed for a KCV Appliance		Security	Group
578	CSR generated for CSP Account {}	M	true	CSR generated for CSP Account		Security	BYOK
579	Azure keyvault {} containing replica keys has purge protection enabled. Rotation operations will fail.	M	true	A vault containing replica keys has purge protection enabled.		Security	BYOK
580	Replication of the key rotation for key {} to vault {} failed. The key must be manually restored to {} and synced in KeyControl to restore redundancy. Review other replica vaults in case replication has not occurred in them either.	H	true	Replication of a key rotation in Azure failed.		Security	BYOK
581	Trial period for vault {} has expired. This vault is now read only. Please connect to CSP Compliance Manager to retrieve a valid license.	H	true	Vault trial period has expired.		Licensing	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
582	{} {} has not been able to connect to CSP Compliance Manager for {} days. This is required for licensing checks. This vault is now read only. Please check the network connectivity and CSP Compliance Manager status.	H	true	Vault grace period has expired.		Licensing	
583	{} {} is unlicensed. No license information is available for {}. This vault is now read only. Check that the vault type is covered by your license.	H	true	No license available for vault.		Licensing	
584	The number of {} {} has exceeded the licensed limit of {}. Current usage: {}. This {} is now read only. Please purchase additional licenses.	H	true	License limit exceeded.		Licensing	
585	The license for {} expired on {}. This vault is now read only. Please renew your license.	H	true	License Expired.		Licensing	
586	Trial period for {} {} is nearing expiration. To avoid loss of service, please connect to CSP Compliance Manager to retrieve a valid license.	M	true	Vault trial period is nearing expiration.		Licensing	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
587	The license for {} will expire on {}. Please renew your license to avoid loss of service.	M	true	License Nearing Expiry.		Licensing	
588	{} {} is in the grace period after upgrade to {} and will become unlicensed when this grace period ends.	M	true	Upgrade Grace Period Nearing Expiry.		Licensing	
589	The number of {} {} is over 90% of the licensed limit of {}. Current usage: {}. To avoid loss of service, please purchase additional licenses if needed.	M	true	Usage is nearing license limit.		Licensing	
590	Attempt to register a new node, named server "%s" failed -- license check failed. Reason: %s.	L	false	Appliance license check failed.		Licensing	
591	Attempt to register a new node, named "%s" failed -- cluster not connected to KeyControl Compliance Manager.	L	false	Appliance is not connected to KCM.		Licensing	
592	Enabled Authentication Inheritance	M	true	Enabled Authentication Inheritance		Security	AUTHENTICATION
593	Disabled Authentication Inheritance	M	true	Disabled Authentication Inheritance		Security	AUTHENTICATION

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
594	Successfully fetched Key Encryption Key from HSM.	H	false	Successfully fetched Key Encryption Key from HSM.		Security	Key Encryption Key
595	OIDC authentication settings updated for Appliance and inheriting vaults	M	true	OIDC authentication settings updated for Appliance and inheriting vaults		Security	AUTHENTICATION
596	OIDC authentication settings for inheriting vault updated by System Admin	M	true	OIDC authentication settings for inheriting vault updated by System Admin		Security	AUTHENTICATION
597	XKS store for {} ({}) in region {} is unreachable	H	true	XKS service unreachable		Security	BYOK
598	XKS store {} ({}) in region {} is {}.	H	true	XKS store not connected		Security	BYOK
599	XKS store {} ({}) in region {} is now CONNECTED.	M	true	XKS store connected		Security	BYOK
600	%s for Virtual Machine %s. %s, reauthentication required.	H	true	%s for Virtual Machine %s. %s, reauthentication required.		Security	
604	Could not pass CSP vault's appliance info to CSP CM {}	L	false	Failed to send CSP vault's appliance info to CSP CM		Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
615	Two-factor authentication enforced by %s	M	false	Two factor authentication has been enforced for the users		Security	
616	Two-factor authentication enforcement removed by %s	M	false	Two factor authentication enforced removed for the users		Security	

CSP Vault for Cryptographic APIs Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for Cryptographic APIs.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a **%s** represents a string value. For example, in the following message:

  Added user **%s** to group **%s**

  The actual message will be displayed with the name of the user and group, for example:

  Added user **fred** to group **IT**

Msg ID	Message	Severity	Alert?	Category
300	{user_name} created the policy '{policy_name}'	M	false	Tokenization
301	{user_name} updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	Tokenization
302	{user_name} deleted the policy '{policy_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
303	{user_name} changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	Tokenization
500	User '{user_name}' logged in successfully.	H	false	Tokenization
400	Cryptographic APIs Client Certificate '{name}' created	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
401	Cryptographic APIs Client Certificate '{name}' created using Certificate Signing Request	M	false	Tokenization
402	Cryptographic APIs Client Certificate '{name}' deleted	M	false	Tokenization
501	Active Directory login for {username} succeeded but failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group base dn in Active Directory configuration might be wrong. Please contact Token Administrator to validate the Active Directory setup.	H	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
502	Login failure for Active Directory user {username} from {client_ip}. Reason: {reason}	H	false	Tokenization
503	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	Tokenization
504	{user_name} enabled authentication inheritance	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
505	Authentication settings for inheriting vault {vault_name} {action} by System Admin	M	false	Tokenization
600	{user_name} updated AD Setting '{ad_setting_name}'	M	false	Tokenization
601	{user_name} changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
602	{user_name} added AD Setting '{ad_setting_name}'	M	false	Tokenization
800	{user_name} updated token '{token_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}.	M	false	Tokenization
801	{user_name} renamed token '{old_name}' to '{token_name}'.	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
802	{user_name} updated tokenization '{token_name}' settings of authentication method to AD based authentication	M	false	Tokenization
803	{user_name} updated tokenization vault '{token_name}' settings about KCM information with 'kcm ip: ' {kcm_ip}.	M	false	Tokenization
804	{user_name} updated tokenization '{vault_name}' settings of authentication method to OIDC based authentication	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
900	{user_name} created the user '{name}'	M	false	Tokenization
901	{user_name} deleted the user '{name}'	M	false	Tokenization
902	{user_name} updated the user '{name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
903	Account {user_name} locked for 5 minutes due to repeated login failures	M	false	Tokenization
904	Account {user_name} disabled due to repeated login failures	M	false	Tokenization
905	Login failure for Local user {username} from {client_ip}. Reason: {reason}	H	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
906	Successfully updated password for user: {username}	H	false	Tokenization
907	Account {user_name} enabled Two-factor authentication	M	false	Tokenization
908	Account {user_name} disabled Two-factor authentication	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
909	{user_name} updated the local user password policy	M	false	Tokenization
910	{user_name} enforced Two-factor authentication	M	false	Tokenization
911	{user_name} enforced Two-factor authentication {user_name} removed enforcement of Two-factor authentication	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1000	{user_name} created keyset '{keyset}'	M	false	Tokenization
1001	{user_name} failed to create keyset: '{message}	M	false	Tokenization
1002	{user_name} enabled HSM for keyset '{keyset}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1003	{user_name} failed to enable HSM. Reason: '{message}'	M	false	Tokenization
1004	{user_name} disabled HSM for keyset '{keyset}'	M	false	Tokenization
1005	{user_name} failed to disable HSM. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1100	{user_name} tokenized data using policy '{policy}'	M	false	Tokenization
1101	{user_name} detokenized data using policy '{policy}'	M	false	Tokenization
1102	{user_name} masked data using policy '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1103	{user_name} detokenized and masked data using policies '{policy}'	M	false	Tokenization
1104	{user_name} encrypted data using key '{key}'	M	false	Tokenization
1105	{user_name} decrypted data using key '{key}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1106	{user_name} failed to tokenize data: '{message}'	M	false	Tokenization
1107	{user_name} failed to detokenize data: '{message}'	M	false	Tokenization
1108	{user_name} failed to mask data: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1109	{user_name} failed to detokenize and mask data: '{message}'	M	false	Tokenization
1110	{user_name} failed to encrypt data: '{message}'	M	false	Tokenization
1111	{user_name} failed to decrypt data: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1112	{user_name} rekeyed data using policies '{policy}'	M	false	Tokenization
1113	{user_name} batch tokenized data using policies '{policy}'	M	false	Tokenization
1114	{user_name} batch detokenized data using policies '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1115	{user_name} batch masked data using policies '{policy}'	M	false	Tokenization
1116	{user_name} batch rekeyed data using policies '{policy}'	M	false	Tokenization
1117	{user_name} failed to rekey data using policies '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1118	{user_name} failed to batch tokenize data using policies '{policy}'	M	false	Tokenization
1119	{user_name} failed to batch detokenize data using policies '{policy}'	M	false	Tokenization
1120	{user_name} failed to batch mask data using policies '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1121	{user_name} failed to batch rekey data using policies '{policy}'	M	false	Tokenization
1122	{user_name} signed data using key '{key}'	M	false	Tokenization
1123	{user_name} verified signature using key '{key}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1124	{user_name} failed to sign data: '{message}'	M	false	Tokenization
1125	{user_name} failed to verify signature: '{message}'	M	false	Tokenization
1126	{user_name} wrapped key using key '{key}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1127	{user_name} unwrapped key using key '{key}'	M	false	Tokenization
1128	{user_name} failed to wrap key: '{message}'	M	false	Tokenization
1129	{user_name} failed to unwrap key: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1130	{user_name} generated mac using key '{key}'	M	false	Tokenization
1131	{user_name} verified mac using key '{key}'	M	false	Tokenization
1132	{user_name} failed to generate mac: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1133	{user_name} failed to verify mac: '{message}'	M	false	Tokenization
1134	{user_name} has generated message digest	M	false	Tokenization
1135	{user_name} failed to generate message digest: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1136	{user_name} batch encrypted data using keys '{keys}'	M	false	Tokenization
1137	{user_name} batch decrypted data using keys '{keys}'	M	false	Tokenization
1138	{user_name} failed to batch encrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1139	{user_name} failed to batch decrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization
1140	{user_name} batch encrypted-decrypted data using keys '{keys}'	M	false	Tokenization
1141	{user_name} failed to batch encrypt-decrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1200	{user_name} created tokenization policy: '{policy}'	M	false	Tokenization
1201	{user_name} deleted tokenization policy: '{policy}'	M	false	Tokenization
1202	{user_name} updated tokenization policy: '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1203	{user_name} created masking policy: '{policy}'	M	false	Tokenization
1204	{user_name} deleted masking policy: '{policy}'	M	false	Tokenization
1205	{user_name} updated masking policy: '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1207	{user_name} deleted encryption policy: '{policy}'	M	false	Tokenization
1209	{user_name} failed to create tokenization policy. Reason: '{message}'	M	false	Tokenization
1210	{user_name} failed to delete tokenization policy. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1211	{user_name} failed to update tokenization policy. Reason: '{message}'	M	false	Tokenization
1212	{user_name} failed to create masking policy. Reason: '{message}'	M	false	Tokenization
1213	{user_name} failed to delete masking policy. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1214	{user_name} failed to update masking policy. Reason: '{message}'	M	false	Tokenization
1216	{user_name} failed to delete encryption policy. Reason: '{message}'	M	false	Tokenization
1300	{user_name} created the key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1301	{user_name} failed to create key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1302	{user_name} updated details of key: '{key_name}'	M	false	Tokenization
1303	{user_name} changed state of the key: '{key_name}' to '{state}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1304	{user_name} scheduled deletion of key: '{key_name}'	M	false	Tokenization
1305	{user_name} cancelled scheduled deletion of key: '{key_name}'	M	false	Tokenization
1306	{user_name} failed to schedule or cancel schedule deletion of key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1307	{user_name} purged key: '{key_name}'	M	false	Tokenization
1308	{user_name} failed to purge key: '{key_name}'	M	false	Tokenization
1309	{user_name} rotated key: '{key_name}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1310	{user_name} failed to rotate key: '{key_name}'	M	false	Tokenization
1311	{user_name} fetched clear value of key: '{key_name}'	M	false	Tokenization
1312	{user_name} failed fetch clear value of key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1313	{user_name} exported key: '{key_name}'	M	false	Tokenization
1314	{user_name} failed to export key: '{key_name}'	M	false	Tokenization
1315	{user_name} generated {key_name} key and CSR	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1316	{user_name} failed to generate {key_name} key and CSR. Reason: '{message}'	M	false	Tokenization
1317	{user_name} exported public key: '{key_name}'	M	false	Tokenization
1318	{user_name} failed to export public key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1319	{user_name} imported key: '{key_name}'	M	false	Tokenization
1320	{user_name} failed to import key: '{key_name}'	M	false	Tokenization
1321	{user_name} has successfully rebuilt keys database	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1322	{user_name} has failed to rebuild keys database. Reason: '{message}'	M	false	Tokenization
1323	{user_name} imported clear key: '{key_name}'	M	false	Tokenization
1324	{user_name} failed to import clear key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1400	{user_name} created Personal Access Token {token_name}	M	false	Tokenization
1401	{user_name} {update_info} Personal Access Token {token_name}	M	false	Tokenization
1402	{user_name} deleted Personal Access Token {token_name}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1500	{user_name} created OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1501	{user_name} failed to create OIDC user {oidc_user_email}	M	false	Tokenization
1502	{user_name} updated OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1503	{user_name} failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1504	{user_name} deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1505	{user_name} failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1506	{user_name} created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1507	{user_name} failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1508	Login failure for OIDC user {username} from {client_ip}. Reason: {reason}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1600	{user_name} cleared cache	M	false	Tokenization
1601	{user_name} failed to clear cache. Reason: '{message}'	M	false	Tokenization
1602	{user_name} changed caching state	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1603	{user_name} failed to change caching state. Reason: '{message}'	M	false	Tokenization
1604	{user_name} fetched caching status	M	false	Tokenization
1605	{user_name} failed to get caching status. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1606	{user_name} fetched caching settings	M	false	Tokenization
1607	{user_name} failed to get caching settings. Reason: '{message}'	M	false	Tokenization
1608	{user_name} set caching settings	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1609	{user_name} failed to set caching settings. Reason: '{message}'	M	false	Tokenization

CSP Vault for KMIP Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for KMIP.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a **%s** represents a string value. For example, in the following message:

  Added user **%s** to group **%s**

  The actual message will be displayed with the name of the user and group, for example:

  Added user **fred** to group **IT**

MsgID	Message	Severity	Alert?	Category
300	{user_name} created the policy '{policy_name}	M	false	KMIP
301	{user_name} updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	KMIP
302	{user_name} deleted the policy '{policy_name}'	M	false	KMIP
303	{user_name} changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	KMIP
400	KMIP Client Certificate '{name}' created	H	false	KMIP
401	KMIP Client Certificate '{name}' created using Certificate Signing Request	H	false	KMIP

MsgID	Message	Severity	Alert?	Category
402	KMIP Client Certificate '{name}' deleted	H	false	KMIP
403	KMIP Client Certificate '{name}' created using uploaded Certificate	H	false	KMIP
500	User '{user_name}' logged in successfully.	H	false	KMIP
501	Active Directory login for {username} succeeded but Kmip portal failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group base dn in Active Directory configuration might be wrong. Please contact Kmip Administrator to validate the Active Directory setup.	H	false	KMIP
502	Login failure for Active Directory user {username}	H	false	KMIP
503	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	KMIP

MsgID	Message	Severity	Alert?	Category
504	{user_name} enabled authentication inheritance	M	false	KMIP
505	Authentication settings for inheriting vault {vault_name} {action} by System Admin	M	false	KMIP
600	{user_name} updated AD Setting '{ad_setting_name}'	M	false	KMIP
601	{user_name} changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	KMIP
602	{user_name} added AD Setting '{ad_setting_name}'	M	false	KMIP
700	KMIP Request - Operation: {op}, Object: {obj}, UUID: {uuid} from KMIP Client - {user} (IP: {client_ip})	H	false	KMIP

MsgID	Message	Severity	Alert?	Category
701	KMIP Response - Operation: {op}, Object: {obj}, UUID: {uuid}, Result: {result}, from KMIP Client - {user} (IP: {client_ip})	H	false	KMIP
702	KMIP Action Request from WebGUI. Action: Revoke, UUID: {uuid}. Revocation Code: {revcode}, Revocation message: {revmsg}, Result: {result} (IP: {client_ip})	H	false	KMIP
703	KMIP Action Response from WebGUI. Action: {op}, UUID: {uuid}, Result: {result} (IP: {client_ip})	H	false	KMIP
800	{user_name} updated kmip '{kmip_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}.	M	false	KMIP
801	{user_name} updated kmip '{kmip_name}' settings of authentication method to AD based authentication with Active Directory domain '{ad_domain}'	M	false	KMIP
802	{user_name} updated kmip '{kmip_name}' settings about KCM information with 'kcm ip: ' {kcm_ip}.	M	false	KMIP

MsgID	Message	Severity	Alert?	Category
803	{user_name} updated kmip '{kmip_name}' settings of authentication method to OIDC based authentication	M	false	KMIP
900	{username} updated KEK Setting	M	false	KMIP
901	{username} enabled KMIP KEK wrapping	M	false	KMIP
902	{username} disabled KMIP KEK wrapping	M	false	KMIP
10000	Successfully completed rekey of KMIP objects	L	false	KMIP
10001	Successfully completed decryption of KMIP objects	L	false	KMIP

MsgID	Message	Severity	Alert?	Category
1002	Successfully started rekey of KMIP objects	L	false	KMIP
1100	Successfully reset KMIP vault {tenant}	L	false	KMIP
1200	{user_name} created the user '{name}'	M	false	KMIP
1201	{user_name} deleted the user '{name}'	M	false	KMIP
1202	{user_name} updated the user '{name}'	M	false	KMIP
1203	Account {user_name} locked for 5 minutes due to repeated login failures	H	false	KMIP

MsgID	Message	Severity	Alert?	Category
1204	Account {user_name} disabled due to repeated login failures	H	false	KMIP
1205	Login failure for Local user {username} from {client_ip}. Reason: {reason}	H	false	KMIP
1206	Successfully updated password for user: {username}	H	false	KMIP
1207	Account {user_name} enabled Two-factor authentication	L	false	KMIP
1208	Account {user_name} disabled Two-factor authentication	L	false	KMIP
1209	{user_name} updated the local user password policy	M	false	KMIP

MsgID	Message	Severity	Alert?	Category
1210	{user_name} enforced Two-factor authentication	M	false	KMIP
1211	{user_name} removed enforcement of Two-factor authentication	M	false	KMIP
1300	{user_name} created Personal Access Token {token_name}	M	false	KMIP
1301	{user_name} {update_info} Personal Access Token {token_name}	M	false	KMIP
1302	{user_name} deleted Personal Access Token {token_name}	M	false	KMIP
1400	{user_name} created OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP

MsgID	Message	Severity	Alert?	Category
1401	{user_name} failed to create OIDC user {oidc_user_email}	M	false	KMIP
1402	{user_name} updated OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1403	{user_name} failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1404	{user_name} deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1405	{user_name} failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1406	{user_name} created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP

Msg ID	Message	Severity	Alert?	Category
1407	{user_name} failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1408	Login failure for OIDC user {username} from {client_ip}. Reason: {reason}	M	false	KMIP

CSP Vault for Secrets Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for Secrets.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the Message column, a %s represents a string value. For example, in the following message:
  Added user %s to group %s
  The actual message will be displayed with the name of the user and group, for example:
  Added user fred to group IT

Msg ID	Message	Severity	Alert?	Category
1	{user_name} created the box '{box_name}'	M	false	Vault
2	{user_name} updated the box '{box_name}'	M	false	Vault
3	{user_name} deleted the box '{box_name}'	M	false	Vault
4	{user_name} revoked the box '{box_name}'	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
100	{user_name} created the secret '{secret_name}' in the box '{box_name}'	M	false	Vault
101	{user_name} updated the secret '{secret_name}' in the box '{box_name}	H	false	Vault
102	{user_name} deleted the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
103	{user_name} revoked the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
104	{user_name} checked out the secret '{secret_name}' from the box '{box_name}'. Secret version is {secret_version}. Lease expiration: {expiration}.	H	false	Vault
105	{user_name} checked in version {secret_version} of secret '{secret_name}' in the box '{box_name}'	H	false	Vault
106	Secret '{secret_name}' in the box '{box_name}' was rotated. New secret version is {secret_version}.	H	false	Vault
107	Rotating the secret '{secret_name}' in the box '{box_name}' failed. Current secret version is {secret_version}.	M	false	Vault
109	{user_name} accessed secret data from the secret '{secret_name}' in the box '{box_name}'. Secret version accessed is {secret_version}.	H	false	Vault
110	{user_name} updated the secret data of the secret '{secret_name}' in box '{box_name}'. New secret version is {secret_version}.	M	false	Vault
111	{user_name} changed the current version of the secret '{secret_name}' in the box '{box_name}'. Current secret version is {secret_version}	M	false	Vault
112	Setting secret '{secret_name}' version {secret_version} in the box '{box_name}' invalid.	M	false	Vault
113	{user_name} appended key certificate pair to the secret '{secret_name}' in the box '{box_name}'.	H	false	Vault

Msg ID	Message	Severity	Alert?	Category
115	{user_name} removed key certificate pair from the secret '{secret_name}' in the box '{box_name}'.	H	false	Vault
200	Lease for the secret '{secret_name}' from the box '{box_name}' checked out by '{checkout_user}' expired	H	false	Vault
201	{user_name} deleted the lease for the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
202	{user_name} renewed the lease for the secret '{secret_name}' from the box '{box_name}'. Secret version is {secret_version}. Lease expires at '{expiration}'.	M	false	Vault
300	{user_name} created the policy '{policy_name}'	M	false	Vault
301	{user_name} updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	Vault
302	{user_name} deleted the policy '{policy_name}'	M	false	Vault
303	{user_name} changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	Vault
400	Secret '{secret_name}' from the box '{box_name}' was not rotated due to outstanding lease(s). Current secret version is {secret_version}.	M	false	Vault
500	User '{user_name}' logged in successfully.	H	false	Vault
501	Active Directory login for {username} succeeded but PASM Vault failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group base dn in Active Directory configuration might be wrong. Please contact Vault Administrator to validate the Active Directory setup.	H	false	Vault
502	Login failure for Active Directory user {username} from {client_ip}. Reason: {reason}	H	false	Vault
503	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	Vault

Msg ID	Message	Severity	Alert?	Category
504	{user_name} enabled authentication inheritance	M	false	Vault
505	Authentication settings for inheriting vault {vault_name} {action} by System Admin	M	false	Vault
600	{user_name} updated AD Setting '{ad_setting_name}'	M	false	Vault
601	{user_name} changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	Vault
602	{user_name} Added AD Setting '{ad_setting_name}'	M	false	Vault
700	{user_name} created the secret rotation job {job_id} for the box '{box_name}'	M	false	Vault
701	Secret rotation job {job_id} started for the box '{box_name}', requested by {user_name}	M	false	Vault
702	Secret rotation job {job_id} completed for the box '{box_name}', requested by {user_name}	M	false	Vault
703	Secret rotation job {job_id} completed for the box '{box_name}', requested by {user_name}. Rotation of {failed_count} Secret(s) failed.	M	false	Vault
704	{user_name} deleted the secret rotation job {job_id} for the box '{box_name}'	M	false	Vault
800	{user_name} updated vault '{vault_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}.	M	false	Vault
801	{user_name} renamed vault '{old_name}' to '{vault_name}'.	M	false	Vault
802	{user_name} updated kmip '{vault_name}' settings of authentication method to AD based authentication with Active Directory domain '{ad_domain}'	M	false	Vault
803	'{user_name}' initiated HSM {op} operation on PASM vault '{vault_name}'.	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
804	'{user_name}' updated HSM DEK cache timeout of PASM vault '{vault_name}' to {period}.	M	false	Vault
805	HSM {state} successfully on PASM vault '{vault_name}'.	M	false	Vault
806	{user_name} updated PASM vault '{pasm_name}' settings about KCM information with 'kcm ip: ' {kcm_ip}.	M	false	Vault
807	{user_name} updated vault '{vault_name}' settings of authentication method to OIDC based authentication	M	false	Vault
900	{user_name} created the user '{name}'	H	false	Vault
901	{user_name} deleted the user '{name}'	H	false	Vault
902	{user_name} updated the user '{name}'	H	false	Vault
903	Account {user_name} locked for 5 minutes due to repeated login failures	H	false	Vault
904	Account {user_name} disabled due to repeated login failures	H	false	Vault
905	Login failure for Local user {username} from {client_ip}. Reason: {reason}	H	false	Vault
906	Successfully updated password for user: {username}	H	false	Vault
907	Account {user_name} enabled Two-factor authentication	M	false	Vault
908	Account {user_name} disabled Two-factor authentication	M	false	Vault
909	{user_name} updated the local user password policy	M	false	Vault
910	{user_name} enforced Two-factor authentication	M	false	Vault
911	{user_name} removed enforcement of Two-factor authentication	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
1000	{user_name} updated kubernetes configuration of '{vault_name}'. 'degraded mode availability' {state}	M	false	Vault
1001	Login failure for Kubernetes user {username} Reason: {reason}	H	false	Vault
1002	Kubernetes User '{user_name}' logged in successfully	H	false	Vault
1100	{user_name} created Personal Access Token {token_name}	M	false	Vault
1101	{user_name} {update_info} Personal Access Token {token_name}	M	false	Vault
1102	{user_name} deleted Personal Access Token {token_name}	M	false	Vault
1200	{user_name} created OIDC user {oidc_user_email}: {oidc_user_guid}'	M	false	Vault
1201	{user_name} failed to create OIDC user {oidc_user_email}'	M	false	Vault
1202	{user_name} updated OIDC user {oidc_user_email}: {oidc_user_guid}'	M	false	Vault
1203	{user_name} failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1204	{user_name} deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1205	{user_name} failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1206	{user_name} created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1207	{user_name} failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1208	Login failure for OIDC user {username} from {client_ip}. Reason: {reason}	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
1301	Approver {approver} {status} the checkout approval request. Request id {request_id}. Comment: {comment}	M	false	Vault
1302	User {user} submitted Checkout approval request for secret {secret_id} in box {box_id}. Approvers {approvers} and minimum approvals required {min_approval}	M	false	Vault
1303	User {user} submitted box secondary approval update request for box {box_id}. Approvers {approvers} and minimum approvals required {min_approval}	M	false	Vault
1304	{user_name} deleted the request '{request_id}'	M	false	Vault
1400	Secret Vault Client Certificate '{name}' created	M	false	Vault
1401	Secret Vault Client Certificate '{name}' created using Certificate Signing Request	M	false	Vault
1402	Secret Vault Client Certificate '{name}' deleted	M	false	Vault

Differences in CSP Vault Audit Messages

The following lists display the differences between audit log messages in CSP Vault.

Differences between v. 10.5.1 and 10.6.1:

- Many audit messages in all categories were updated for grammatical and coding errors.

Differences between v. 10.4.7 and 10.5.1:

- New audit messages in main audit file: 563-567, 571-576, 579-600, 604, 615-616
- Updated audit messages in main audit file: 251-252, 418-419, 429-434, 457, 488, 497, 506, 514-515, 533, 577
- New audit messages in CSP Vault for Cryptographic APIs: 504-505, 910-911, 1323-1324, 1136-1141
- Updated audit messages in CSP Vault for Cryptographic APIs: 400-402, 1205, 1214,
- New audit messages in CSP Vault for KMIP: 504-505, 1210-1211
- New audit messages in CSP Vault for Secrets: 504-505, 910-911

Differences between v. 10.4.5 and 10.4.7:

- New audit messages in main audit file: 561-562, 568-570, 577-578
- New audit messages in CSP Vault for Cryptographic APIs: 1134-1135, 1321-1322
- New audit messages in CSP Vault for Secrets: 1400-1402

Differences between v. 10.4.3 and 10.4.5:

- New audit messages in main audit file: 548-560
- New audit messages in CSP Vault for Cryptographic APIs: 400-402, 1600-1609

Differences between v. 10.4.1.1 and 10.4.3:

- New audit messages in main audit file: 539-547
- Updated audit messages: 538

Differences between v. 10.3.3 and 10.4.1.1:

- Separate audit logs were created for the CSP Vault for Cryptographic APIs, the CSP Vault for KMIP, and the CSP Vault for Secrets. The main audit file contains audit logs for the KeyControl Vault Management Appliance, the CSP Vault for Cloud Keys, the CSP Vault for Databases, and the CSP Vault for VM Encryption.
- New audit messages: 479, 525-538
- Updated audit messages: 386, 456, 480

14 Customer license

This section defines the licensing model and permitted uses of the Entrust Cryptographic Security Platform (CSP) software solution.

Authorized Use

In this Licensing Model section, the term "Customer" means an Entrust customer who has purchased one or more CSP software licenses, or an individual authorized by that customer to access components or capabilities of the CSP software ("Users").

CSP software is licensed for internal Customer use (i.e., use for the Customer's own business purposes). Customer may also grant access to Users who are employees of external contractors, but only to the extent that such Users are using CSP software on Customer's behalf in the operation or management of the Customer's business and Customer's own cryptographic assets. In addition, the Customer is permitted to provide digital certificates to Users outside the Customer's organization solely to enable communications and resource access between the Customer and that User.

Except as may be otherwise specified in an express license agreement signed by Entrust, neither Customer nor any User may use CSP software to set up or provide its own cryptographic management, analysis, or reporting service for other companies (e.g., provision of CSP software functionality as a "Managed Service Provider" or "Systems Integrator").

License

The Customer will receive one or more license keys ("licenses") to enable CSP software functionalities and volumes of Keys and Secrets, certificates, and Third-party Objects based on what the Customer has purchased.

The CSP software solution is offered with a base licensing package (Entrust CSP On -Premise Core) that can be extended with add-on licenses for specific capabilities and volumes.

Base Licensing Package: Entrust CSP on Premise Core

Inclusions	**Excluded/Separate License Required**
Compliance Manager: 2-node cluster	Additional Compliance Manager nodes require separate add-on licenses (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster*)

Inclusions	Excluded/Separate License Required
Standard Compliance Pack: assessment, documentation, and risk scoring for Discovery scan results and one additional data source (e.g., Vault Cluster, Certificate Manager, KeySafe 5).	Additional data sources require a separate add-on license (*Entrust CSP ADD-ON Compliance Manager - Standard Assessment, Documentation, and Risk Scoring (per Vault Cluster)*). Discovery scan results do not count as a data source for licensing purposes.
Discovery (scanning)	
KeySafe 5 (HSM manager)	
File Encryption – 10 GB	The 10 GB protected data limit is calculated based on the original data size and excludes any overhead (added data size) resulting from the encryption. Licensing beyond 10 GB requires a separate license (per Terabyte per year) (*Entrust CSP ADD-ON File Encryption Subscription 1TB*). NOTE: Disc Encryption for Virtual Machines (Linux/Windows) requires a separate Vault Cluster (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults)* and Virtual Machines volume licenses (*Entrust CSP ADD-ON Virtual Machine Encryption Keys Subscription*)

Add-on Licenses

Capabilities	Add-on licenses	Notes/Consumption
Compliance Management	Third-party Objects (*Entrust CSP ADD-ON Integration with Third Party KMS Keys Subscription*)	Volume-based license, consumed when a Third Party Object is imported into Compliance Manager inventory, as follows: Active Object = 1 full license Inactive Object but still managed = 1/10 of a license (dormant object) Deleted Object, or unmanaged object = no license required
	Compliance Manager nodes (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster*)	Additional 2 nodes for higher availability or multiple clusters – Compliance Manager supports up to a maximum of 8 nodes per cluster.

Capabilities	Add-on licenses	Notes/Consumption
	Standard Compliance Pack: assessment, documentation, and risk scoring (*Entrust CSP ADD-ON Compliance Manager - Standard Assessment, Documentation, and Risk Scoring (per Vault Cluster)*)	Every Vault Cluster, Certificate Manager, KeySafe 5, needs its own Standard compliance Pack.
HSM Management	KeySafe 5 Monitoring (*nShield - KeySafe 5 Monitoring Base*, *nShield - KeySafe 5 Monitoring Standard*, *nShield - KeySafe 5 Monitoring Mid*, or *nShield - KeySafe 5 Monitoring Enterprise*)	Tier-based license determined by the number of HSMs being monitored and subject to an annual (12-month) subscription.
Certificate Management	Certification Authority (*Entrust CSP ADD-ON Certification Authority*)	Certificates require separate licensing.
	Advanced PKI (*Entrust CSP ADD-ON Advanced PKI*)	Timestamping Authority software (included in Advanced PKI) may be deployed as a three-node cluster, limited to up to 600 timestamps per second (TPS).
	Advanced CLM (Entrust CSP ADD-ON Advanced CLM)	
	Timestamping Expansion (*Entrust CSP ADD-ON Timestamping Expansion*)	Expansion of Timestamping Authority (included in Advanced PKI) by two additional nodes or increase the limit on existing nodes by up to an additional 600 TPS. The maximum number of nodes per cluster is 5.
	Certificates (*Entrust CSP ADD-ON Production Certificates*)	Volume-based license. A certificate license is required for each active certificate.
Keys and Secrets Management	Vault Cluster: 2-node cluster (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults*)	Each license covers a single 2-node cluster. A Vault Cluster supports up to a maximum of 8 nodes.

Capabilities	Add-on licenses	Notes/Consumption
	KMIP Keys *(Entrust CSP ADD-ON KMIP Keys Subscription)*	Each of these is a volume-based license, consumed as follows: Active Key/Secret = 1 full license Inactive Key/Secret but still managed = 1/10 of a license (dormant Key/Secret) Deleted Key/Secret, or unmanaged Key/Secret = no license required
	Secrets *(Entrust CSP ADD-ON Managed Secrets Keys Subscription)*	
	Cloud Keys *(Entrust CSP ADD-ON Bring Your Own Key, Hold Your Own Key, and Native Key Mgmt Keys Subscription)*	
	TDE Databases *(Entrust CSP ADD-ON TDE Database Keys Subscription)*	
	Application Keys *(Entrust CSP ADD-ON Application Security inc. Tokenization and Cryptographic Rest API Keys Subscription)*	
	Virtual Machines Keys *(Entrust CSP ADD-ON Virtual Machine Encryption Keys Subscription)*	

These licenses are subject to the following terms:

- For items purchased on a volume basis, Customer may not exceed the total volume indicated in the applicable purchased license. If Customer's consumption exceeds the licensed volume entitlements that it has purchased, Entrust may invoice Customer an overage fee in arrears for its actual consumption.
- The Customer may not alter the license key or attempt to circumvent the licensing mechanism.
- The Customer may only use a valid license key provided by Entrust with the corresponding CSP software component.

Deployment

CSP software may be deployed on the Customer's own infrastructure and/or commercial cloud environments. Entrust strongly recommends keeping all deployments up to date with the latest product release.

External Dependencies

CSP software licenses do not include any Hardware Security Modules (HSM). These components are external dependencies that must be provided, installed, and configured separately by the Customer before the CSP software can operate.

Trade Compliance

CSP software contains cryptographic software components. The Customer's country of operation may have import and export requirements that apply.

Standard Compliance Packs Limitations

The Standard Compliance Packs included with CSP Compliance Manager (each a “Compliance Pack” and collectively the “Compliance Packs) are provided to assist organizations in reviewing their cryptographic keys, secrets, and certificates against industry standards and best practices. While these Compliance Packs will assist the Customer, Entrust does not represent, warrant, or guarantee that their use will ensure, guarantee, or confirm compliance with any particular industry standards and best practices or any specific policy, regulation, or other laws. The Customer is solely responsible for validating all requirements and managing compliance with all relevant industry standards and best practices or any specific policy, standard, or regulation, or other laws (and to determine which of these are applicable to its activities). Entrust disclaims any and all liability arising from Customer's reliance on the Compliance Packs.

Support and Record-Keeping

To ensure Entrust Customer Support is equipped to assist with reported issues, the Customer is expected to maintain reasonable records of CSP software deployment details, including the production instances in use and the environment(s) (on-premises or cloud) where those instances reside. In addition, upon Entrust's request, Customer will provide a report detailing its consumption of Keys and Secrets, certificates, and Third-party Objects.

15 Programmer's Reference Guide

hicli Scripting Guide

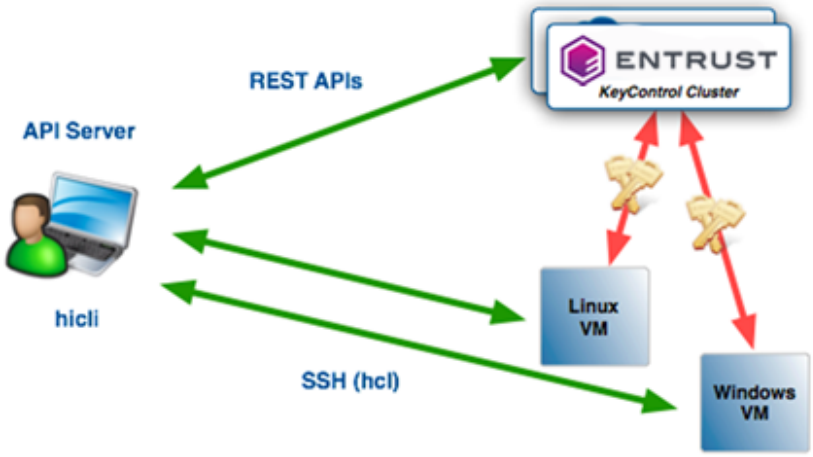
Introduction

This chapter describes `hicli`, which can be used for managing operations between the Cryptographic Security Platform Vault cluster and a Entrust Policy Agent present in Linux and Windows virtual machines. `hicli` uses a combination of the Cryptographic Security Platform Vault REST APIs to communicate with Cryptographic Security Platform Vault, and SSH to invoke `hcl` commands on Windows and Linux VMs.

The Policy Agent provides for encryption of devices within Linux and Windows virtual machines. The management of keys and the administration of the Policy Agent is through a Cryptographic Security Platform Vault cluster. Administration can take place through the webGUI, through the RESTful APIs, or through using the `hicli` command.

hicli can only be accessed through the Cryptographic Security Platform Vault for Databases webGUI and the Cryptographic Security Platform Vault for VM Encryption webGUI.

The following figure shows the servers that are involved:



We will be operating with one or more clustered Cryptographic Security Platform Vault nodes, a number of Linux or Windows VMs and the API Server, a server from which `hicli` will be invoked. This can be almost any UNIX-like server including Linux, BSD variants, OS/X and so on.

Installing and Configuring hicli

`hicli` is available in an API bundle from the Cryptographic Security Platform Vault webGUI:

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download Policy Agent**.
4. From the Available Downloads dialog box, download the `hcs-api-10.5.3-buildnum.tgz` file, where `buildnum` is the build number for the release you are installing.
5. Copy the `tgz` file to the VM on which you want to install the API.
6. Navigate to a directory where you want to install the package and untar it as follows:
   $ cd ~
   $ tar xvfz hcs-api-10.5.3-*buildnum*.tgz

   x hcs-api/
   x hcs-api/hclcomm.py
   x hcs-api/kpsapi.py
   x hcs-api/docopt.py
   x hcs-api/hicli
7. `hicli` needs the Python `requests` module, and to manage Windows VMs, it also needs the `winrm` module. Install these modules:
   $ pip install requests
   $ pip install pywinrm

8. Set up `PYTHONPATH` to point to the new directory and modify your `PATH` so that the shell can reference the `hicli` program. For example, if the install location is `/Users/spate`, the environment variables need to be set up as follows:
   $ export PYTHONPATH=$PYTHONPATH:/Users/spate/hcs-api
   $ export PATH=$PATH:/Users/spate/hcs-api

   Note: If your python installation only includes a python command and not a python3 command, then do one of the following:
   - Edit the first line of hicli from `#!/usr/bin/env python3 to #!/usr/bin/env python`.
   - Define an alias similar to `hicli='python /Users/<user_name>/hcs-api/hicli'` using your install location.
9. Set up a configuration file named `~/.hicli/hicli.cfg` that contains information about the virtual machines to be managed. The following example shows a configuration file with two Linux VMs and one Windows VM.
   Notes:
   - The number and location of curly brackets is important. Make sure your configuration file looks like the example below.
   - If the platform is not specified it defaults to `"linux"`.
   - A password is required for Windows platforms to connect over winrm.
   - By default, the `hicli.cfg` file is used to resolve VM names. If no entries are found, DNS is used to resolve the VM names.
   - On Linux, you can run `hicli` commands as `root` or as a `sudo` user. If you specify a `sudo` user, you also specify a password if the `sudo` user requires one. On Windows, you can run `hicli` with any Windows account that has Administrator privileges.

   The following example shows a `hicli.cfg` file with three Linux VMs and one Windows VM. The Linux ubuntu10.04 VM uses the standard `root` account, the ubuntu12.10 VM uses the `sudo` user `spate` with the password `DogDays123!`, and the rhel73 VM uses the passwordless `sudo` user `jsmith`. The Windows VM uses the `Administrator` account with the password `XYZ@123`.

```
{
 "cvmlist": {
  "ubuntu10.04": {
   "host":"192.168.140.129",
   "port":"22",
   "user":"root"
  },
  "ubuntu12.10": {
   "host":"192.168.140.130",
   "port":"22",
   "user":"spate",
   "sudo_password" : "DogDays123!"
  },
  "rhel73": {
   "host":"192.168.140.131",
```

```
    "port":"22",
    "user":"jsmith"
   },
   "Windows2012r2": {
    "host":"192.168.140.132",
    "user":"Administrator",
    "password":"XYZ@123",
    "platform": "windows"
   }
  }
}
```

If you want to manage another VM with `hicli`, just add that entry to the `cfg` file.

```
{
 "cvmlist": {
   "ubuntu10.04": {
    "host":"192.168.140.129",
    "port":"22",
    "user":"root"
   },
   "ubuntu12.10": {
    "host":"192.168.140.130",
    "port":"22",
    "user":"spate",
    "sudo-password" : "DogDays123!"
   },
   "rhel73": {
    "host":"192.168.140.131",
    "port":"22",
    "user":"jsmith"
   },
   "Windows2012r2": {
    "host":"192.168.140.132",
    "user":"Administrator",
    "password":"XYZ@123",
    "platform": "windows"
```

```
  },
  "ubuntu13.04": {
    "host":"192.168.140.133",
    "port":"22",
    "user":"root"
  }
 }
}
```

10. To verify the installation, run the `hicli` command and you should see a comprehensive listing of the command and its options.
11. To set up SSH communication on each Linux host, generate a key pair on the API server and copy the public key to each VM on which you want to run API commands. The public key should be appended to the `authorized_keys` file for either `root` or the sudo user you specified in the `hicli.cfg` file. (For the Windows VM you would use WinRM.)
    The following example uses `ssh-keygen` on the API server to generate the key pair and then uses `ssh-copy-id` to send the public key to the Linux VMs we added to the `hicli.cfg` file above.

```
api# cd ~/.ssh
api# ssh-keygen -t dsa
api# ssh-copy-id id_dsa.pub root@192.168.140.129
api# ssh-copy-id id_dsa.pub spate@192.168.140.130
api# ssh-copy-id id_dsa.pub jsmith@192.168.140.131
api# ssh-copy-id id_dsa.pub root@192.168.140.133
```

    After you copy the public key to the VM, make sure that, on each VM:
    - You enable **root** or sudo user login over SSH to the VM. If you are using a passwordless sudo user, you need to set up passwordless SSH access for that user using the pub.
    - You turn off SSH warnings.

    To test that SSH access is working between your API server and your VM, issue a test command over SSH. For example, you can use SSH to query the hostname on the VM:

```
$ ssh root@192.168.140.129 hostname
ubuntu10.04
```

hicli Command Categories

Category	Base Commands	Notes

Domain Management	`domain`
	`mapping`
	`server`
		These commands configure your Cryptographic Security Platform Vault servers and Cluster Node Mappings.
		Accessibility: DOMAIN_ADMIN
		Details: Domain Management

Category	Base Commands	Notes
Group Management	`group`	This command creates and manages the user groups in the system. Accessibility: SEC_ADMIN. Other users can list, and view details for, only those groups of which they are a member. Details: Cloud Admin Group Management
User Management	`user`	This command creates and manages the Cryptographic Security Platform Vault user accounts in the system. Accessibility: SEC_ADMIN. Other users can access the details of their own user account only. Details: User Management
Cloud VM Set Management	`cvmset` `global`	The `cvmset` command allows you to create and manage individual Cloud VM Sets. The `global` command lets you specify default parameters to be used when a new Cloud VM Set is created. Accessibility: CLOUD_ADMIN, but that CLOUD_ADMIN must belong to the Cloud Administration group associated with the Cloud VM Set they are trying to manage. Details: Cloud VM Set Management
VM Management	`cvm`	The `cvm` command lets you manage the VMs registered with the Cloud VM Sets defined in the system. Accessibility: Accessibility: CLOUD_ADMIN, but that CLOUD_ADMIN must belong to the Cloud Administration group associated with the Cloud VM Set with which the VM is registered. Details: VM Management
KMIP Server Object Management	`kmipsrv_obj`	This command lets you retrieve and manage the objects stored in the Entrust KMIP server. Details: KMIP Server Object Management
AWS (Amazon Web Services) buckets	`s3`	This command lets you create and manage S3 buckets. Accessibility: GUEST_ADMIN Details: AWS S3 Bucket Management

Category	Base Commands	Notes
Alerts	`alert`	This command lets you view and delete alerts. Accessibility: All users can view or delete the alerts sent to their user account. Details: Alert Management

Selecting a CSP Vault Node

Cryptographic Security Platform Vault nodes are typically clustered. Before invoking `hicli` commands, you must first select a Cryptographic Security Platform Vault node to talk to. If you have a cluster of two or more nodes, it does not matter which Cryptographic Security Platform Vault node is chosen. Since the nodes operate in an active-active cluster, any change to any node is immediately reflected on all nodes in the cluster.

You select a node as follows:

```
$ hicli kc select kc-1
$ hicli kc
Current CSP Node: kc-1
$ hicli kc select 192.168.140.152
$ hicli kc
Current CSP Node: 192.168.140.152
```

DNS is used to resolve hostnames, so either be sure to set up DNS for all your Cryptographic Security Platform Vault nodes, or use IP addresses, as shown above.

Domain Management

`hicli` Command	Description
`domain detail`	Display information about a domain
`domain list`	Display all domains
`domain select`	Select a domain
`domain set allow_reconnect`	Display information about a domain
`domain set description`	Give the domain a new description

`hicli` Command	Description
`domain set hide_passphrase`	Don't display the passphrase when adding a new node
`domain set require_passphrase`	Require a passphrase when adding a new node
`generate_csr`	Generates a CSR (Certificate Signing Request) that you can send to a CA (Certificate Authority) to generate a custom certificate.
`mapping list`	Displays the Cluster Node Mappings configured in the domain.
`mapping new`	Creates a new Node Mapping.
`mapping detail`	Displays details about the specified Node Mapping.
`mapping rm`	Removes the specified Node Mapping.
`mapping select`	Sets the Node Mapping to which future commands will be applied.
`mapping set description`	Sets the Node Mapping description.
`mapping set group`	Sets the Administration Group with which this mapping will be associated.
`mapping set servers`	Sets the IP addresses of the Cryptographic Security Platform Vault nodes in this Node Mapping.
`mapping set newname`	Changes the Node Mapping name.
`server auth`	Display information about a domain.
`server default_csr_values`	Displays the default CSR values for the named server.
`server detail`	Display detailed information about a server.
`server install_cert`	Installs a custom certificate on the server.

`hicli` Command	Description
`server install_cert_status`	Displays information about the status of the certificate installation process.
`server show_cert`	Shows the current server certificate.
`server use_default_certs`	Tells Cryptographic Security Platform Vault to ignore any custom certificates and to return to using the default, self-signed Cryptographic Security Platform Vault certificate.
`server webserver_restart`	Restarts the web server on the Cryptographic Security Platform Vault node. This is required after you install a new custom certificate.

Cryptographic Security Platform Vault Node Examples

The `domain list` command shows the name of the Cryptographic Security Platform Vault domain:

```
$hicli domain list
Domain                Admin Group                Servers   Status
-------------------------------------------------------------------------
KeyControl Domain     KeyControl Admin Group     1         Healthy
```

And now get details about the Cryptographic Security Platform Vault domain:

```
$ hicli domain detail "KeyControl Domain"
Name                 KeyControl Domain
Status               Healthy
Group                KeyControl Admin Group
Description          Domain of Clustered KeyControl Servers
Allow reconnect      Yes
Passphrase required  Yes
Passphrase hidden    No
Check hardware id    Yes
Server Count         2
Server Names         kc1.hytrust.com,kc2.hytrust.com
```

To set Cryptographic Security Platform Vault domain attributes:

```
$ hicli domain set "KeyControl Domain" --description="New description" \
   --allow_reconnect=yes --require_passphrase=yes \
   --hide_passphrase=no
```

For Cryptographic Security Platform Vault server operations we need to select the domain first:

```
$ hicli domain select "KeyControl Domain"
```

To show the Cryptographic Security Platform Vault domain is selected:

```
$ hicli domain
KeyControl Domain
```

Get Cryptographic Security Platform Vault server details:

```
$ hicli server detail kc1.hytrust.com
Name          kc1.hytrust.com
```

```
Status         Online
IP Address     192.168.140.151
Authenticated  Yes
```

Authenticate the Cryptographic Security Platform Vault server:

```
$ hicli server auth kc1.hytrust.com
```

Cluster Node Mapping Examples

List the Cluster Node Mappings already defined in the domain:

```
$ hicli mapping list
KeyControl Mapping Name   Admin Group          Description
-------------------------------------------------------------------------------
kc-west-coast-mapping     Cloud Admin Group    KC servers on the west coast
```

Create a new Cluster Node Mapping:

```
$ hicli mapping new kc-east-coast-mapping "Cloud Admin Group"
"kc1:192.168.13.124:443,kc2:192.168.12.157:443" --description="KC servers on the east coast"
```

Verify that the new Node Mapping was created:

```
$ hicli mapping list
KeyControl Mapping Name   Admin Group          Description
-------------------------------------------------------------------------------
kc-east-coast-mapping     Cloud Admin Group    KC servers on the east coast
kc-west-coast-mapping     Cloud Admin Group    KC servers on the west coast
```

Get the details for a Cluster Node Mapping:

```
$ hicli mapping detail kc-east-coast-mapping
Name           | kc-east-coast-mapping
Admin Group    | Cloud Admin Group
Description    | KC servers on the east coast
servers        | "kc1:192.168.13.124:443:0.0.0.0:1,kc2:192.168.12.157:443:0.0.0.0:1"
```

Change the servers in the Node Mapping. Note that the list you specify overwrites the existing list, so if you want to add a server to the existing list, you must specify all servers that are already in the list as well as the one you want to add.

```
$ hicli mapping set kc-east-coast-mapping --servers
"kc1:192.168.13.124:443,kc2:192.168.12.157:443,kc3:192.168.11.162:443"
```

Select and the view the selected Node Mapping:

```
$ hicli mapping select kc-east-coast-mapping
$ hicli mapping
Current KeyControl Mapping: kc-east-coast-mapping
```

Delete a Node Mapping, then select the mapping to make sure it has been removed:

```
$ hicli mapping rm kc-east-coast-mapping
$ hicli mapping select kc-east-coast-mapping
KeyControl Mapping not found: kc-east-coast-mapping
```

Cryptographic Security Platform Vault Certificate Examples

Generate a CSR (Certificate Signing Request):

```
$ hicli generate_csr --common_name=kc1.hytrust.com --country=US --days=180 --state=California
--locality="San Francisco" --org=HyTurst --org_unit=Engineering
--sans="kc2.hytrust.com,kc3.hytrust.com,kc4.hytrust.com"
```

Show the text of the certificate named `mycert.pem`:

```
$ hicli server show_cert mycert.pem
```

Install the custom certificate `mycert.pem` on the Cryptographic Security Platform Vault node `kc1.hytrust.com`. After you install the certificate you must restart the webserver on the node.

> Note: If the certificate was generated using the CSR created by the `hicli generate_csr` command, you do not need to specify a private key file or password.

```
$ hicli server install_cert kc1.hytrust.com --cert_file=mycert.pem --cacert=mycacert.pem
$ hicli server webserver_restart kc1.hytrust.com
```

Install a custom certificate `my-other-cert.pem` on the Cryptographic Security Platform Vault node `kc2.hytrust.com`. This certificate was generated using a custom CSR command, so you must also specify the private key file and password (if required).

```
$ hicli server install_cert kc2.hytrust.com --cert_file=my-other-cert.pem --private_key=key.pem
--password=DogDays123! --cacert=my-other-cacert.pem
$ hicli server webserver_restart kc1.hytrust.com
```

Return to using the default, self-signed Cryptographic Security Platform Vault certificate:

```
$ hicli server use_default_certs kc1.hytrust.com
```

Cloud Admin Group Management

All commands are available to SEC_ADMINs. Other users can view only those Cloud Admin Groups of which they are a member. They cannot make any changes to those groups.

`hicli` Command	**Description**
`group list`	List the Cloud Admin Groups defined in Cryptographic Security Platform Vault.
`group new`	Create a new Cloud Admin Group.
`group detail`	View the details for the selected Cloud Admin Group.
`group rm`	Remove the selected Cloud Admin Group. Tip: One common problem is that, even after you remove all the users from a group, group removal fails because the group is still associated with one or more Cloud VM Sets. To avoid this, make sure you remove all associations between the group and any Cloud VM Sets *before* you remove the users. At that point you can remove the group.

`hicli` Command	Description
`group add_user`	Add a Cryptographic Security Platform Vault-managed user account to the selected Cloud Admin Group. This user account must already be defined in Cryptographic Security Platform Vault.
`group rm_user`	Remove a Cryptographic Security Platform Vault-managed user account from the selected Cloud Admin Group.
`group set` *description*	Change the description for the selected Cloud Admin Group.
`group set name`	Change the name of the selected Cloud Admin Group.

Examples

> Note: In the following examples, the responses shown for the `hicli group list` command are truncated to display just the group name and membership lists. The full output shows additional details for the Cloud Admin Groups such as the group description and whether the group can be deleted from Cryptographic Security Platform Vault.

View the current set of Cloud Admin Groups:

```
$ hicli group list
Group Name          | AD Group Members                    | User Members
-------------------------------------------------------------------------------------------
Cloud Admin Group   | Azure Admins                        | secroot
```

Display more detailed information about a specific group:

```
$ hicli group detail "Cloud Admin Group"
Name                | Cloud Admin Group
Description         | Default Group for Administering Cloud VMs
Type                | CLOUD_ADMIN
Number of objects   | 0
AC Policy Max Changes | 50
User Members        | secroot
AD Group Members    | Azure Admins
```

Create a new Cloud Admin Group called `cld_group1` and add the AD Security group `AWS Admins` to that Cloud Admin Group:

```
# hicli group new cld_group1 --privilege=CLOUD_ADMIN --adgroup_members='[{"distinguishedName":
"CN=AWS Admins,CN=Users,DC=manualtest,DC=qa,DC=dc,DC=hytrust,DC=com", "objectGUID":
"29739b20-2fb2-4b99-b7a8-935560b5c8f4", "cn": "AWS Admins"}]'
#
# hicli group list
Group Name          | AD Group Members                    | User Members
-------------------------------------------------------------------------------------------
Cloud Admin Group   | Azure Admins                        | secroot
cld_group1          | AWS Admins                          |
```

Change the AD Security group membership for `cld_group1` to `VMware Admins`. This command removes any existing AD group members from the Cloud Admin Group.

```
# hicli group set cld_group1 --adgroup_members='[{"distinguishedName": "CN=VMware
Admins,CN=Users,DC=manualtest,DC=qa,DC=dc,DC=hytrust,DC=com", "objectGUID":
"b2e5d325-1d2c-455a-b2ee-9408fd9e4841", "cn": "VMware Admins"}]'
#
# hicli group list
Group Name          | AD Group Members                          | User Members
-------------------------------------------------------------------------------------------
Cloud Admin Group    | Azure Admins                             | secroot
cld_group1          | VMware Admins                             |
```

User Management

All commands are available to SEC_ADMINs. Other users can only set some details for their own user account.

`hicli` Command	**Description**
`user list`	View the list of Cryptographic Security Platform Vault users defined in the system. SEC_ADMIN sees all users. Others see users in the user groups to which they belong.

`hicli` Command	Description
`user new username`	Creates a new user account with the specified username. You can also specify the following properties: • `--email=<email>` • `--password=<passwd>` • `--full_name=<full_name>` • `--authentication=<authentication>` — The default authentication method. This can be `local` or `ldap`. This option affects only newly-created user accounts. It does not change the authentication method for existing accounts. • `--account_state=<active|disabled>` • `--roles=<privlist>` — The allowed roles are: `CLOUD_ADMIN`, `DOMAIN_ADMIN`, `SEC_ADMIN`, or any combination of the three. Separate multiple role names with commas. For example: `--roles=SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN`. If you are changing the roles for a user, you must specify all roles you want the user to have. For example, if the user currently has CLOUD_ADMIN privileges and you specify `--roles=SEC_ADMIN`, the user will now have only SEC_ADMIN privileges and will be removed from any Cloud Administration groups they may have been associated with. To add the SEC_ADMIN role, you would specify `--roles=CLOUD_ADMIN,SEC_ADMIN`. • `--groups=<grouplist>` — The groups to which this user should belong. Each group name must be surrounded by " (double quotes). Separate multiple group names with commas. For example: `--groups="Cloud Admin Group","Domain Admin Group"`. • `--password_expiration=<date>` — The date on which the selected user's password expires. The next time that user logs in, they will be prompted to set a new password. • `--account_expiration=<date>` — The date on which the user account will be automatically disabled. You can re-enable the account at any time after it has expired using `--account_state=active`.
`user set username`	Set information for the specified user. SEC_ADMIN can set all information for all accounts. Other users can only set the email address, full name, and password for their own account. You can specify any or all of the properties that can be specified for a new user account.
`user detail username`	View the details for the specified user. SEC_ADMIN can view the details for any user. Others can only view the details for their own user account.

`hicli` Command	Description
`user rm username`	Removes the specified user.
`user defaults`	Set the default parameters for Cryptographic Security Platform Vault user accounts. You can specify: • `authentication` — The default authentication method. This can be `local` or `ldap`. This option affects only newly-created user accounts. It does not change the authentication method for existing accounts. • `password_expiry` — The number of days before the user's password expires. This option affects only newly-created accounts. It does not change the password expiration date for existing accounts. • `max_failed_logins` — The number of failed login attempts that can be made before Cryptographic Security Platform Vault disables the user account. This setting affects all user accounts, including existing accounts. • `min_passwd_length` — The minimum number of characters required in a Cryptographic Security Platform Vault account password. This setting affects all user accounts, including existing accounts.

Set User Defaults Example

The following example sets the default authetication to local, the password expriation to 60 days after the account is created or the password is changed, the maxium failed login attempts to 4, and the minimum password lenght to 12 characters.

```
$ hicli user defaults --authentication=local --password_expiry=60 \
    --max_failed_logins=4 --min_passwd_length=12
```

For other user management examples, see:

- Examples: Logging In and Viewing Users
- Examples: Creating and Modifying Users
- Examples: Removing Users

Examples: Logging In and Viewing Users

To login into Cryptographic Security Platform Vault, invoke `hicli` as follows:

```
$ hicli user login secroot Password for secroot: ********
```

If you don't specify the `--password=` option you will be prompted for it on the command line.

After logging in, a user context is set such that all subsequent operations will be performed as that user. To show which user is currently logged on, run the following command:

```
$ hicli user
Currently logged-on user: secroot
```

You can also request details about yourself as follows:

```
$ hicli user detail secroot
Login name              | secroot
Status                  | Active
Full name               | Security Administrator
Email                   | spate@me.com
Last login              | 2018-04-13 10:22:15 PDT
Password Expiration     | Never
Account Expiration      | Never
Failed logins           | 0
Privileges              | SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
Groups                  | Domain Admin Group, KeyControl Admin Group,\
                        | Cloud Admin Group
$ hicli user login spate
Password for spate: ********
$ hicli user detail spate
Login name              | spate
Status                  | Active
Full name               | Steve Pate
Email                   | spate@me.com
Last login              | 2018-04-13 10:21:03 PDT
Password Expiration     | Never
Account Expiration      | 06/09/2020
Failed logins           | 0
Privileges              | CLOUD_ADMIN
Groups                  | Cloud Admin Group
```

Once you have finished a current session, you can log out as follows:

```
$ hicli user
Currently logged-on user: spate
$ hicli user logout
$ hicli user
Login first
```

Examples: Creating and Modifying Users

The following example selects one of the Cryptographic Security Platform Vault nodes, logs in as secroot, lists the users and groups, and then creates two new users, one called `spate` with the same privileges as secroot and one called `mrogers` with just the CLOUD_ADMIN user role in the `West-Cloud-Group` Cloud Admin Group.

```
$ hicli kc select kc-1
$ hicli kc
Current KeyControl: kc-1
$ hicli user login secroot
Password for secroot: ********
$ hicli user list
Username    Full Name             Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
$ hicli group list
Group Name          Description                    Members
-------------------------------------------------
```

```
Cloud Admin Group       Default Group for Administering Cloud VMs   secroot
West-Cloud-Group        Includes all West Coast Cloud VM Sets       secroot
$ hicli user new spate --email=spate@me.com --password=Mypasswd236! \
    --roles="SEC_ADMIN, DOMAIN_ADMIN, CLOUD_ADMIN" --full_name="Steve Pate" \
    --groups="Cloud Admin Group, SF-Datacenter"
$ hicli user new mrogers --email=martha@me.com --password=Passwd123! \
    --roles="CLOUD_ADMIN" --full_name="Martha Rogers" --groups="SF-Datacenter"
$ hicli user list
Username    Full Name             Privileges
-------------------------------------------------
mrogers     Martha Rogers         CLOUD_ADMIN
secroot     Security Administrator  SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
spate       Steve Pate            SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
$ hicli group list
Group Name            Description                         Members
-----------------------------------------------
Cloud Admin Group       Default Group for Administering Cloud VMs   secroot,spate
West-Cloud-Group        Includes all West Coast Cloud VM Sets       secroot,spate,mrogers
```

If there is more than one Cryptographic Security Platform Vault node in the cluster, you can select any node. As soon as changes are made on one node, they are automatically reflected on all other nodes. In the example here, we have selected kc-1.

Since we are creating a new user, we must first log on as a Security Administrator. In the example above, we were prompted for the password. Alternatively, you can specify the password on the command line using `--password=`. Login sessions are valid for one hour past the last command typed. We recommend that sets of commands be preceded by a login call and followed by a logout call.

In order to check the progress of your API calls, log on to the webGUI and view the results.

Modifying a User Example

As an example, consider the following user:

```
$ hicli user detail fred
Login name              | fred
Status                  | Active
Full name               | Fred Flintstone
Email                   | fred@me.com
Last login              | 2018-04-13 10:21:03 PDT
Password Expiration     | Never
Account Expiration      | 06/09/2020
Failed logins           | 0
Privileges              | CLOUD_ADMIN
Groups                  | Cloud Admin Group
```

The following call adds Security Admin privileges and changes the email:

```
$ hicli user set fred --roles=SEC_ADMIN,CLOUD_ADMIN --email=fred@hytrust.com
$ hicli user detail spate
Login name              | fred
Status                  | Active
Full name               | Fred Flintstone
Email                   | fred@hytrust.com
Last login              | 2018-04-13 10:21:03 PDT
Password Expiration     | Never
```

```
Account Expiration      | 06/09/2020
Failed logins           | 0
Privileges              | SEC_ADMIN,CLOUD_ADMIN
Groups                  | Cloud Admin Group
```

Examples: Removing Users

Only Security Administrators can remove users. In the example below, we display the current list of users and then remove the user spate. We then re-run the command to confirm that the removal took place. Note that you need to specify the username.

```
$ hicli user list
Username    Full Name             Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN
spate       Steve Pate              CLOUD_ADMIN
$ hicli user rm spate
$ hicli user list
Username    Full Name             Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN
```

Note that all objects (Cloud VM Sets and VMs) are owned by administrative groups and not by the users themselves. Thus, if you remove a user, the object will stay intact.

Cloud VM Set Management

Cloud VM Sets are managed by administrators with CLOUD_ADMIN privileges. The administrator must be a member of the Cloud Admin Group that is associated with the Cloud VM Set.

The table below shows the Cloud VM Set operations.

`hicli` Command	**Description**
`cert detail`	Display information about the specified certificate. For examples, see Examples: Cloud VM Set Certificates.
`cert new`	Create a new certificate for the Cloud VM Set.
`cert rm`	Remove an unused certificate.
`cvmset`	Display current Cloud VM Set.
`cvmset detail`	Display details about the specified Cloud VM Set.
`cvmset kek_edit`	Change the settings for the KEK (Key Encryption Key) associated with the Cloud VM Set. For examples, see Examples: Cloud VM Sets with the KEK Feature.

`hicli` Command	Description
`cvmset kek_state_change`	Revoke or unrevoke the KEK.
`cvmset list`	List all Cloud VM Sets.
`cvmset list_tasks`	Display list of tasks for the specified Cloud VM Set.
`cvmset new`	Create a new Cloud VM Set. For examples, see Examples: Creating and Changing Cloud VM Sets.
`cvmset select`	Select a Cloud VM Set.
`cvmset set`	Change properties.
`cvmset set grace`	Set the value for the grace period in seconds (default is 1 day).
`cvmset set heartbeat`	Set the value for the heartbeat in seconds (default is 5 minutes, or 300 seconds).
`cvmset set name`	Change the name of the Cloud VM Set.
`cvmset set rekey`	Set the value for the automatic rekey of disks interval in days/months/years (defaults to 0 which means not set).
`cvmset set rekeybucket`	Set the value for the rekeybucket for cvmset which controls the max number of auto rekeys that can be processed in parallel. Auto rekey is triggered when rekey interval expires. This value defaults to 1.
`global set`	Set the defaults for newly-created Cloud VM Sets. Changing these options does not affect any existing Cloud VM Sets. You can specify: • `--heartbeat` — The default value for the heartbeat in seconds (default is 5 minutes, or 300 seconds). • `--grace` — The value for the grace period in seconds (default is 1 day).
`keyid new`	Create a KeyID. For examples, see Examples: KeyIDs.
`keyid rm`	Remove a KeyID.

hicli Command	Description
keyid revoke	Revoke access to a KeyID.
keyid set expiration	Set the expiration date for a KeyID.
keyid set onexpiry	When a KeyID expires, set the expiration policy.
keyid unrevoke	Unrevoke access to a KeyID.

Examples

List the existing Cloud VM Sets:

```
$ hicli cvmset list
Cloud VM Set Name     Admin Group          Description
-------------------------------------------------
Amazon AWS            Cloud Admin Group    VMs sets sited on Amazon Servers
vCloud Air            Cloud Admin Group    VMs sets deployed on vCloud Air \
                                           servers
Sales Staff           Cloud Admin Group    Sales staff worldwide
```

Set global default settings:

```
$ hicli global set --heartbeat=60 --grace=600
```

For other Cloud VM Set management examples, see:

- Examples: Creating and Changing Cloud VM Sets
- Examples: Cloud VM Sets with the KEK Feature
- Examples: Cloud VM Set Certificates
- Examples: KeyIDs

Examples: Creating and Changing Cloud VM Sets

Below, we create a new Cloud VM Set called Amazon-EC2 then check to make sure that it has been created:

```
$ hicli cvmset new "Amazon-EC2" "Cloud Admin Group" --description="VMs running in Amazon
Ubuntu-10.04,linux-12.10"
$ hicli cvmset list | grep Amazon-EC2
Amazon-EC2            Cloud Admin Group    VMs running in Amazon Ubuntu-10.04,linux-12.10
```

You can view details about an existing Cloud VM Set as follows:

```
$ hicli cvmset detail "Amazon-EC2"
Name                  Amazon-EC2
Admin Group           Cloud Admin Group
Guid                  d4a7093a-185e-11e8-a8fd-000c2997200a
Description           VMs running in Amazon Ubuntu-10.04,linux-12.10
```

Unused Certificate Ids 4c81a042a60b11e2b5cf000c29ed8423
KeyIDs aws_key,test_key

To change properties use the `hicli cvmset set` command. For example:

$ `hicli cvmset set "Amazon-EC2" --description="Amazon Southwest"`

More attributes (default Heartbeat and Grace Period) may be specified using Cloud VM Set creation and modification:

```
$ hicli cvmset new "Amazon-EC2" "Cloud Admin Group" \
   --description="Amazon Southwest" --heartbeat=60 --grace=600
$ hicli cvmset set "Amazon-EC2" --group="Cloud Admin Group" \
   --description="Rackspace" --heartbeat=60 --grace=600
```

Examples: Cloud VM Sets with the KEK Feature

A Key Encryption Key (KEK) provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with a Cloud VM Set. Both the KEK and the individual data encryption key must be available before the information on the VM can be accessed.

If you want to use a KEK with a Cloud VM Set, you can either specify it during Cloud VM Set creation or add it later.

If you use a KEK, all of the VMs in the Cloud VM Set share the expiration date and expiration options specified for the KEK.

For details about using a KEK with a Cloud VM Set, see KEKs with Cloud VM Sets.

Create a new Cloud VM Set with a KEK:

```
$ hicli cvmset new "kek_cvmset" "Cloud Admin Group" --cvm_set_type='KEK_ASSOC'
   --kek_expire_days=10 --kek_expire_action='NO USE'--expiration_options=change
   --retention_period=2
```

Add a KEK to an existing Cloud VM Set:

$ hicli cvmset add_kek “kek_cvmset" —kek_expire_days=12 —kek_expire_action="NO USE” —expiration_options=extend

Change the configuration options for a KEK. This command requires the guid for the Cloud VM Set.

```
$ hicli cvmset kek_edit 30dd18df-185f-11e8-a8fd-000c2997200a --kek_expire_days=14
    --kek_expire_action=SHRED --expiration_options=no_change
```

When you edit KEK options, keep the followings in mind:

- If you change the date on which a KEK expires using the `--kek_expire_days` parameter, the new expiration date is calculated from the date on which you run the command, not from the original expiration date.
- If the KEK expiration option is set to SHRED, the KEK will be destroyed immediately upon reaching the expiration date. You cannot extend the date for a KEK if it has been shredded. If the KEK expiration option is set to NO_USE, the expiration date can be extended after the KEK expires and the KEK can be reactivated.

Revoke access to all VMs in the Cloud VM Set immediately, regardless of the expiration date associated with the KEK:

$ hicli cvmset kek_state_change 30dd18df-185f-11e8-a8fd-000c2997200a REVOKE

Restore access to all VMs in the Cloud VM Set immediately, as long as the KEK associated with the Cloud VM Set has not expired:

$ hicli cvmset kek_state_change 30dd18df-185f-11e8-a8fd-000c2997200a UNREVOKE

Examples: Cloud VM Set Certificates

A Key Encryption Key (KEK) provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with a Cloud VM Set. Both the KEK and the individual data encryption key must be available before the information on the VM can be accessed.

If you want to use a KEK with a Cloud VM Set, you can either specify it during Cloud VM Set creation or add it later.

If you use a KEK, all of the VMs in the Cloud VM Set share the expiration date and expiration options specified for the KEK.

For details about using a KEK with a Cloud VM Set, see KEKs with Cloud VM Sets.

Create a new Cloud VM Set with a KEK:

$ hicli cvmset new "kek_cvmset" "Cloud Admin Group" --cvm_set_type='KEK_ASSOC'
--kek_expire_days=10 --kek_expire_action='NO USE'--expiration_options=change
--retention_period=2

Add a KEK to an existing Cloud VM Set:

$ hicli cvmset add_kek "kek_cvmset" —kek_expire_days=12 —kek_expire_action="NO USE" —
expiration_options=extend

Change the configuration options for a KEK. This command requires the guid for the Cloud VM Set.

$ hicli cvmset kek_edit 30dd18df-185f-11e8-a8fd-000c2997200a --kek_expire_days=14
--kek_expire_action=SHRED --expiration_options=no_change

When you edit KEK options, keep the followings in mind:

- If you change the date on which a KEK expires using the `--kek_expire_days` parameter, the new expiration date is calculated from the date on which you run the command, not from the original expiration date.
- If the KEK expiration option is set to SHRED, the KEK will be destroyed immediately upon reaching the expiration date. You cannot extend the date for a KEK if it has been shredded. If the KEK expiration option is set to NO_USE, the expiration date can be extended after the KEK expires and the KEK can be reactivated.

Revoke access to all VMs in the Cloud VM Set immediately, regardless of the expiration date associated with the KEK:

$ hicli cvmset kek_state_change 30dd18df-185f-11e8-a8fd-000c2997200a REVOKE

Restore access to all VMs in the Cloud VM Set immediately, as long as the KEK associated with the Cloud VM Set has not expired:

$ hicli cvmset kek_state_change 30dd18df-185f-11e8-a8fd-000c2997200a UNREVOKE

Examples: KeyIDs

For KeyID operations, a Cloud VM Set has to be selected:

```
$ hicli cvmset select "Amazon EC2"
```

Create a KeyID:

```
$ hicli keyid new aws_key --description "Key for Amazon"
```

Create a KeyID using the encryption algorithm AES-XTS-512 and a custom Base64 encryption key and iv (initialization vector). Note: The Base64 key has been truncated in the following example. When you create the keyid, make sure you specify the full encryption key.

```
$ hicli keyid new custom_key --description "This uses my Base64 key" --crypto_algo='AES-XTS-512'
--key="Q0NOdkJBQWZROUd6emhvRFU1a ... Bb0hJN2RYaQ==" --iv="MTIzNDU2Nzg5MDEyMzQ1Ng==" --
expiry=1000 --onexpiry='SHRED'
```

List KeyIDs:

```
$ hicli keyid list
Key Name    | Description            | Algorithm
-----------------------------------------------------
aws_key     | Key for Amazon         | AES-256
custom_key  | This uses my Base64 key  | AES-XTS-512
```

Show KeyID details:

```
$ hicli keyid detail aws_key
Description      Key for Amazon
Algorithm      AES-256
Expires      Never
Onexpiry      Shred
Status         Active
```

Fetch a KeyID. Note: The Base64 key has been truncated in the following example. `hicli` will return the full Base64 encryption key.

```
$ hicli keyid fetch custom_key
key value      | Q0NOdkJBQWZROUd6emhvRFU1a ... Bb0hJN2RYaQ==
iv value       | MTIzNDU2Nzg5MDEyMzQ1Ng==
```

Change KeyID attributes:

```
$ hicli keyid set aws_key --expiration="12/31/2015" --onexpiry=no_use
```

Revoke a KeyID:

```
$ hicli keyid revoke aws_key
```

Change KeyID attributes:

```
$ hicli keyid set aws_key --expiration="12/31/2015" --onexpiry=no_use
```

Unrevoke a KeyID:

```
$ hicli keyid unrevoke aws_key
```

Remove a KeyID:

```
$ hicli keyid rm aws_key
```

VM Management

The table below shows the VM operations that can be performed on any VM in a Cloud VM Set. All operations can be performed by Cloud Administrators.

`hicli` Command	Description
`cvm add_disk`	Add a disk to be encrypted
`cvm decrypt_task`	Perform decryption on specified disk
`cvm detail`	Get the status of the VM (KeyControl perspective)
`cvm detail_disk`	Display details about a specified disk
`cvm encrypt_task`	Perform encryption on specified disk
`cvm list`	List the VMs in the current Cloud VM Set
`cvm list_tasks`	Display list of tasks for the specified VM
`cvm new`	Add a new VM
`cvm reauth`	Re-authorize a VM
`cvm rekey_task`	Perform rekey on specified disk
`cvm renew clone`	Clone a VM certificate
`cvm revoke`	Revoke access to the VM and its devices
`cvm revoke_disk`	Revoke access to the specified disk
`cvm rm`	Remove a VM
`cvm rm_disk`	Remove a disk from HyTrust management
`cvm s3 add_file`	Add a file to an S3 bucket
`cvm s3 get_file`	Retrieve a file from an S3 bucket

`hicli` Command	Description
`cvm s3 rm_file`	Remove a file from an S3 bucket
`cvm set`	Set properties of the VM
`cvm set rekey`	Set the value for the automatic rekey of disks interval in days/months/years (defaults to 0 which means not set)
`cvm set_disk expiration`	Set the expiration date for a disk
`cvm set_mapping`	Set KC mapping
`cvm status`	Get the status of the VM (as in `hcl status`)
`cvm unrevoke_disk`	Give permissions back to access the device

All of these operations are performed in the context of a Cloud VM Set. So, before invoking any of these commands, you need to set the Cloud VM Set first. Let's first look at the current Cloud VM Set:

```
$ hicli cvmset
Current Cloud VM Set: Amazon EC2
```

You can change the current Cloud VM Set as follows:

```
$ hicli cvmset select "Amazon AWS"
$ hicli cvmset
Current Cloud VM Set: Amazon AWS
```

To list the VMs associated with a Cloud VM Set:

```
$ hicli cvm list
VM Name             Status
-------------------------------------------------
ubuntu-10.04         Online
ubuntu-12.10         Online
```

To request more information about a specific VM, there are two options. The first is equivalent to running `hcl status` on the VM. For example:

```
$ hicli cvm status ubuntu-12.10
Host Status on ubuntu12.10
-------------------------------------------------
Summary
-------------------------------------------------
KeyControl: kc-1:443
KeyControl list: kc-1:443
Status: Connected
```

```
Registered Devices
-------------------------------------------------
Disk Name        Clear                    Cipher     Status
-------------------------------------------------
sdb2           /dev/mapper/clear_sdb2          AES-256     Attached
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sdb1           /dev/mapper/clear_sdb1          AES-256     Attached
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices
-------------------------------------------------
Disk Name        Device Node              Size (in MB)
-------------------------------------------------
sde              /dev/sde                 2048
sdd              /dev/sdd                 2048
sdc              /dev/sdc                 2048

Other Devices
-------------------------------------------------
Disk Name        Device Node              Status
-------------------------------------------------
sda5             /dev/sda5                Mounted (swap)
sda1             /dev/sda1                Mounted (/)
```

And the second displays abbreviated information:

```
$ hicli cvm detail ubuntu-12.10
KeyControl Status for ubuntu12.10
-------------------------------------------------
Name                    ubuntu12.10
IP Address              192.168.11.93
Status                  Online
Description
Cloud VM Set            HCS
OS                      Linux ubuntu 2.7.32-38-generic #83-Ubuntu
            SMP Wed Jan 4 11:12:07 UTC 2014 x86_64 GNU/Linux
Agent version           10.5.3
Valid till              02/01/2020
Heartbeat (sec)         10
Grace period (sec)      3600
Reauth on H/W signature change  Yes
Reauth on IP address change     Yes
Reauth on reboot        No

Disks:
sdb1                    ACTIVE
sdb2                    ACTIVE
```

Adding a new VM and adding devices to be encrypted is very straightforward, as the following script shows:

```
$ hicli user login spate --password=********
$ hicli cvmset set 'Amazon EC2'
$ hicli cvm new ubuntu10.04
$ hicli cvm ubuntu10.04 add_disk sdb1
$ hicli cvm ubuntu10.04 add_disk sdb2
```

We log on to the KeyControl as user spate. Next we select the Cloud VM Set into which we wish to place the VM. The `new` subcommand is used to register and authenticate the new VM. We then add two disks. Note that we are using the abbreviated names sdb1 and sdb2 in place of `/dev/sdb1` and `/dev/sdb2`.

The `hicli cvm new` command involves calling the KeyControl to create and download a new certificate which is then copied to the VM. It then calls `hcl register` from the VM and completes authentication. The call to `add_disk` is the equivalent of `hcl add`, which adds and attaches the device including getting access to the key. Following the call to `add_disk`, the encrypted device is now ready to use.

Note: The Policy Agent software must be installed prior to adding the VM.

At this point, you can view the effects of your script through the Cryptographic Security Platform Vault webGUI.

To undo the effects of the script above, to remove the devices, and to remove the VM, use the following script:

```
$ hicli cvmset select "Amazon EC2"
$ hicli cvm ubuntu-10.04 rm_disk sdb1
$ hicli cvm ubuntu-10.04 rm_disk sdb2
$ hicli cvm revoke ubuntu-10.04
$ hicli cvm rm ubuntu-10.04
```

At this point it will look like the original script was never run.

The `revoke` and `unrevoke` options allow you to forcibly remove access to clear-text data and then grant permissions back to a device. The following operation is equivalent to selecting the Cloud icon, choosing a virtual machine and disk, and then selecting Actions > Revoke Disk Access:

```
$ hicli cvm ubuntu-10.04 revoke_disk sdb2
```

The following operation is equivalent to selecting a device and selecting Actions > Grant Disk Access in the Cryptographic Security Platform Vault webGUI.

```
$ hicli cvm ubuntu-10.04 unrevoke_disk sdb2
```

The `revoke` sub-command is equivalent to selecting a device and then selecting Actions > Revoke VM Authentication in the Cryptographic Security Platform Vault webGUI.

```
$ hicli cvm revoke ubuntu-10.04
```

The opposite operation is the `reauth` of the VM. This will perform the equivalent of running `hcl auth` on the command line of the VM and then typing the passphrase in the webGUI.

```
$ hicli cvm reauth ubuntu-10.04
```

Renew the certificate of a Cloud VM:

```
$ hicli cvm renew ubuntu-12.10
```

Clone a Cloud VM:

```
$ hicli cvm clone ubuntu-12.10 ubuntu-clone
```

Get details of a disk:

```
$ hicli cvm ubuntu-12.10 detail_disk sdb1
Name          sdb1
Mapped Device      clear_sdb1
```

```
Status          Active
Algorithm       AES-256
Expiration      Never
OnExpiry        Shred
Size (bytes)    104857600
```

Change disk attributes:

```
$ hicli cvm ubuntu-12.10 set_disk sdb1 --expiration="12/31/2022" --onexpiry="No Use"
```

Rekey a disk:

```
$ hicli cvm ubuntu-12.10 rekey_disk sdb1
```

Encrypt a file:

```
$ hicli cvm ubuntu-12.10 encryptfile -k aws_key /tmp/files.zip
```

Decrypt a file:

```
$ hicli cvm ubuntu-12.10 decryptfile /tmp/files.zip.enc
```

KMIP Server Management

hicli Command	**Description**
kmipsrv set	Enables, disables, or changes the KMIP server settings. • --state=<ENABLED|DISABLED> —Whether the KMIP server is enabled or disabled. • --host=<ip address> —The IP address of the KMIP server. • --port=<port number> —The port number for the KMIP server. • --reconnect=<0|1> —Whether automatic reconnection is enabled (1) or disabled (0). • --protocol=<1.0|1.1|1.2|1.3|1.4|*custom_hex*> —The KMIP protocol to use for the server. • --nbio=<0|1> —Whether non-blocking I/O is required (1) or not required (0). • --timeout=<timeout> —The length of time, in seconds, after which a client request will time out. Specify 0 (zero) to indicate that the request should never time out. • --verify=<yes|no> —If set to yes, the KMIP client identity is verified before the server handles its request. We recommend that you set this option to yes. • --reset —Resets the KMIP server. • --loglevel=<ALL|CREATE-GET|OFF> —The log level to use for the KMIP server. • --cert_type=<DEFAULT|CUSTOM> —The certificate type being used by the KMIP server. • --SSL_cert=<*path*> —The path of the SSL certificate (in base64 PEM format) to be used. Required if --cert_type is CUSTOM. • --CA_cert=<*path*> —The path of the CA certificate (in base64 PEM format) to be used. Required if --cert_type is CUSTOM. • --private_key=<*path*> —The path of the private key (in base64 PEM format) to be installed. Required if --cert_type is CUSTOM and you did not use a CSR generated by Cryptographic Security Platform Vault. • --custom_cacert_use_to_verify_kmip_client_cert=<0|1> —If enabled, the user must upload a custom certificate while creating the KMIP client certificate. Required if --cert_type is CUSTOM. • --password=<password> —The password of the private key. Required only if the private key is encrypted.

`hicli` Command	Description
`kmipsrv_user`	Creates, edits, or deletes a KMIP Client Certificate bundle: • `--username=<user name>` —The user name for the KMIP client certificate bundle. • `--passwd=<password>` —An optional password for the client certificate bundle. Note that not all KMIP clients can accept a password-protected client certificate. • `--expire=<integer>` —The number of days before the KMIP certificate expires. • `--p12=<yes>` • `--operation=<create|update|remove|removeall|list>` —The operation to preform on the client certificates. • `--csr=<csrfile>` —Optional. The name of the file containing the 3rd party certificate signing request (CSR) you want to use. • `--download` —If specified, the selected client certificate bundle is returned by this command.

KMIP Server Object Management

`hicli` Command	Description
`kmipsrv_obj fetch`	Retrieves a list of objects stored on the KMIP server. You can specify the following properties: • `--uuid=<object uuid>` —The UUID of the KMIP server object. If this parameter is not specified, the command returns a list of the KMIP objects on the server. • `--noattr` —Only include the object UUIDs in the returned list. If this parameter is not specified, this command returns the full details about each KMIP object. `hicli` ignores this option if you specify a UUID. • `--count=<list size>` —The number of KMIP objects to retrieve. • `--offset=<offset>` —The index of the first object to retrieve in the list. If you specify `0` (zero) for this parameter, the command starts at the top of the list. • `--total_count` —Include the total number of objects stored on the KMIP server in the response.

`hicli` Command	Description
`kmipsrv_obj action uuid`	Performs one or more of the following actions on the KMIP server object whose UUID is specified in the command. • `--operation=<activate|archive|destroy|recover|revoke>` —The action to perform on the KMIP object. • `--revcode=<revoke reason code>` —If you are revoking the object, this is the standard KMIP reason code. • `--revmsg=<revoke message>` —If you are revoking the object, this is a user-defined string specifying the reason why you are revoking the object. • `--desc=<description>` —Sets the user-defined description for the object.

Getting a List of KMIP Objects

The following command gets the total number of KMIP objects stored on the server:

```
$ hicli kmipsrv_obj fetch --total_count
Total number of KMIP objects: 10
```

The following command retrieves the details for the first 4 objects:

```
$ hicli kmipsrv_obj fetch --count=4 --offset=0
Object UUID                          Type        State      Initial Date              Last Change               Identification
Description
------------                         ----        -----      ------------              -----------               --------------
------------
bec40e89-e2c9-11e8-9997-000c299ae5eb  PublicKey    PreActive   2018-11-07T20:14:35+00:00
2018-11-07T20:14:35+00:00    []             None
bec39ac3-e2c9-11e8-9997-000c299ae5eb  PrivateKey   PreActive   2018-11-07T20:14:35+00:00
2018-11-07T20:14:35+00:00    []             None
997dd60b-e2c9-11e8-9997-000c299ae5eb  PublicKey    PreActive   2018-11-07T20:13:32+00:00
2018-11-07T20:13:32+00:00    []             None
996b5f4c-e2c9-11e8-9997-000c299ae5eb  PrivateKey   PreActive   2018-11-07T20:13:32+00:00
2018-11-07T20:13:32+00:00    []             None
```

The following command gets only the UUIDs for the first four KMIP objects:

```
$ hicli kmipsrv_obj fetch --count=4 --offset=0 --noattr
bec40e89-e2c9-11e8-9997-000c299ae5eb
bec39ac3-e2c9-11e8-9997-000c299ae5eb
997dd60b-e2c9-11e8-9997-000c299ae5eb
996b5f4c-e2c9-11e8-9997-000c299ae5eb
```

The following command gets a specific KMIP object. Note that even though the `--noattr` option is specified, it is ignored by `hicli`.

```
$ hicli kmipsrv_obj fetch --uuid=997dd60b-e2c9-11e8-9997-000c299ae5eb --noattr
CryptographicUsageMask  :  Encrypt Verify
InitialDate             :  2018-11-07T20:13:32+00:00
State                   :  PreActive
CryptographicAlgorithm  :  RSA
LastChangeDate          :  2018-11-07T20:13:32+00:00
```

```
CryptographicLength     : 4096
ObjectType              : PublicKey
```

Managing KMIP Objects

You can use the following command to manage any KMIP object on the server using that object's UUID:

```
hicli kmipsrv_obj action <uuid> [--operation=<activate|archive|destroy|recover|revoke>]
[--revcode=<revoke_code>] [--revmsg=<revoke_message>] [--desc=<description>]
```

You can perform the following operations on a KMIP server object:

- `activate` —By default, objects are created in PreActive state. Specify `activate` to enable more transitions for the object. **Note:** Many KMIP clients change objects to Active state as part of the creation process.
- `archive` —Objects will no longer return keys but they remain in the system. You can use the `recover` operation to return an archived object to active state and retrieve its keys.
- `destroy` —This operation permanently removes the object. Destroyed objects cannot be retrieved.
- `recover` —Restores an Archived object to the active state so that its keys can be retrieved.
- `revoke` —Revocation is permanent. Objects that are revoked cannot be moved back to Active, but the client can still retrieve any key material. You can also specify a revocation reason, which can be any string, and a numeric Reason Code, which is one of the following KMIP standard codes. If you omit the reason code or use a non-standard code, it will be considered the same as "1—Unspecified."
  1—Unspecified
  2—Key Compromise
  3—CA Compromise
  4—Affiliation Changed
  5—Superseded
  6—Cessation of Operation
  7—Privilege Withdrawn

The following command activates a KMIP object:

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=activate
success
```

The following commands archive and then restore a KMIP object, fetching the details after each action to make sure the state was correctly changed. After you restore an object, the ArchiveDate is retained, but the Archived flag is no longer set.

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=archive
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
Archived              : 1
CryptographicUsageMask  : Decrypt Sign
InitialDate           : 2018-11-07T20:29:19+00:00
State                 : Active
ActivationDate        : 2018-11-09T20:22:18+00:00
ArchiveDate           : 2018-11-09T20:27:05+00:00
CryptographicAlgorithm  : RSA
LastChangeDate        : 2018-11-09T20:27:05+00:00
CryptographicLength     : 4096
ObjectType            : PrivateKey
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=restore
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
```

```
CryptographicUsageMask  :  Decrypt Sign
InitialDate             :  2018-11-07T20:29:19+00:00
State                   :  Active
ActivationDate          :  2018-11-09T20:22:18+00:00
ArchiveDate             :  2018-11-09T20:27:05+00:00
CryptographicAlgorithm  :  RSA
LastChangeDate          :  2018-11-09T20:27:05+00:00
CryptographicLength     :  4096
ObjectType              :  PrivateKey
```

The following command revokes a KMIP object for the revocation reason "This key has been replaced with a new key":

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=revoke --revcode=5
--revmsg='This key has been replaced with a new key'
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
ActivationDate          :  2018-11-09T20:22:18+00:00
RevocationReasonCode    :  Superceded
CryptographicUsageMask  :  Decrypt Sign
InitialDate             :  2018-11-07T20:29:19+00:00
DeactivationDate        :  2018-11-09T20:31:24+00:00
RevocationMessage       :  This key has been replaced with a new key
State                   :  Deactivated
CryptographicAlgorithm  :  RSA
LastChangeDate          :  2018-11-09T20:31:24+00:00
CryptographicLength     :  4096
ObjectType              :  PrivateKey
```

AWS S3 Bucket Management

Amazon Web Services (AWS) S3 buckets can be managed by any account with AWS GUEST_ADMIN privileges.

`hicli` Command	**Description**
`s3 add_file`	Add a file to the S3 bucket.
`s3 rm_file`	Remove a file from the S3 bucket.
`s3 get_file`	Retrieve a file from the S3 bucket.
`set aws_access_key_id`	Set the AWS access key ID.
`set aws_secret_access_key`	Set the AWS shared secret.
`create_bucket`	Create a new S3 bucket.

hicli Command	Description
delete_bucket	Delete an existing S3 bucket.
list_bucket	View the list of available buckets.

Alert Management

All users can list or remove their own alerts. They cannot access the alerts sent to other users.

hicli Command	Description
alert list	List the alerts sent to the logged-in user account.
alert detail *alertnum*	View the details for the specified alert.
alert rm *alertid*	Remove an alert sent to the logged-in user account.

Examples

Get all alerts for the user:

```
$ hicli alert list
1 10/08/17 17:06:52 Account disabled for spate due to repeated failures
2 10/08/17 17:08:00 VM Set Admin Group group has been granted access to datastore dedup on
```

Get the details of alert 1:

```
$ hicli alert detail 1
ID        b62c3bb3954611e3bfe6080027cbdf2a
Message   Account disabled for spate due to repeated failures
Date      10/08/17 17:06:52
```

Delete alert 1:

```
$ hicli alert rm b62c3bb3954611e3bfe6080027cbdf2a
```

Man Page Reference

- hcl Man Page
- htroot Man Page
- hcs3 Man Page

hcl Man Page

NAME

hcl - Encrypt disks, filesystems and files using HyTrust DataControl

SYNOPSIS

hcl [OPTIONS]

DESCRIPTION

The hcl command is used to manage encrypted disks, filesystems and files on Linux and Windows.

OPTIONS

The options are as follows:

General Status

status

Display the list of KeyControl cluster nodes that this VM can communicate with, the status of the connection and the list of encrypted folders/disks and available disks.

status [-g] (Linux only)

Displays partition information about the available disks showing the partition type and the existence of any disk GUID.

Registration

register [-c] [-h myname] [-d description] [-p certificate_password] [-o one_time_passphrase] kc_hostname[:port],kc_hostname2[:port2],... /path/to/cert.bin"

Registers the VM with a KeyControl cluster. This method requires you to authenticate the VM with KeyControl using a one-time passphrase. If you want to use simplified registration, see the "register -a" version of this command described below.

The -c option indicates the presence of a clone certificate so should only be specified if you are registering a clone VM.

The -h option allows you to give a name to the VM which will be visible in the webGUI as well as through APIs.

The -d option allows you to specify an optional description for the VM. This will also be visible in the webGUI as well as through APIs.

The -p option allows you to specify the password for the certificate if one was specified when the certificate was created in the KeyControl webGUI. If you omit this option and a password is required, you will be prompted to enter it.

The -o option allows you to enter a one-time passphrase that you can use to authenticate this VM in the KeyControl webGUI. If you do not specify the -o option, you will be prompted to enter it. This passphrase must contain at least 16 alphanumeric characters or hyphens. The one-time passphrase will be expired after 15 minutes.

"kc_hostname" is a comma-separated list of KeyControl cluster nodes and, optionally, port numbers. The default port is 443. To enable automatic failover, you should enter the IP address of every KeyControl node in the cluster. For example, if you have a three node cluster, you would enter

192.168.162.133,192.168.162.135,192.168.162.137.

Note that if you add or remove any nodes, you should run the "hcl updatekc" command to update this list. Alternatively, if you have set up a KeyControl mapping, you can enter a single IP address and then select a KeyControl mapping when prompted.

The final argument is the pathname to the certificate.

register -a [-c] [-h myname] [-d description] [-n mapping] [-N] [-u username [-s password] [-e certificate expiration] [-v vault_id] [-z cvmset] kc_hostname[:port],kc_hostname2[:port2],...

Registers the VM using simplified registration, with which you do not need to manually create a certificate and copy it to the VM or enter a one-time passphrase. You can quickly register and authenticate a VM by providing your KeyControl credentials, selecting the Cloud VM Set and optional KeyControl mapping.

The -c option allows you to register this VM as clone of the original VM.

The -h option allows you to give a name to the VM which will be visible in the webGUI as well as through APIs.

The -d option allows you to specify an optional description for the VM. This will also be visible in the webGUI as well as through APIs.

The -n option allows you to specify a KeyControl mapping for the VM. If KeyControl has mappings available for the specified Cloud Admin, and this option is omitted, the list of mappings will be displayed and you will be prompted to select one. If you choose to associate the VM with a mapping, the KeyControl list will be automatically updated when the VM heartbeats against the cluster.

The -N option allows you to skip KeyControl mapping for the VM. If this option is provided, the mapping list will not be displayed even if -n is omitted. If both -n and -N options are set, -n option will be ignored.

The -v option allows you to specify a Vault ID for the vault. If you do not specify a vault_id, you will be prompted to enter it.

The -z option allows you to specify the name of the Cloud VM Set to which the VM should be registered. If this option is omitted, you will be prompted to choose the Cloud VM Set from the list of available Cloud VM Sets.

The -e option allows you to specify the certificate expiration date using the format MM/DD/YYYY. For example, 12/25/2017. If an expiration date is not specified, the certificate will be valid for one year from the date of creation.

The -u and -s options allow you to specify a KeyControl user account name and password with Cloud Admin privileges. If you do not specify credentials, or if you specify the user name but not the password, you will be prompted to enter this information.

kc_hostname is a comma-separated list of KeyControl cluster nodes and, optionally, port numbers. The default port is 443. To enable failover, you should enter the IP address of every KeyControl node in the cluster. For example, if you have a three node cluster, you would enter

192.168.162.133,192.168.162.135,192.168.162.137.

Note that if you add or remove any nodes, you should run the "hcl updatekc" command to replace this list. Alternatively, if you have set up KeyControl mappings, you can enter a single IP address and then select a KeyControl mapping when prompted.

unregister [-y] [-a [-u username -p password]]

Unregisters an authenticated VM from KeyControl. If the VM is unregistered successfully, then the local state on the VM is cleaned up. All HyTrust configuration about all disks and folders is removed. This has the effect of uninstalling and re-installing the product and should be used with extreme caution.

When dealing with VM clones, Do Not use this command unless VM is registered as a clone (refer 'hcl register') to avoid any accidental data loss.

The -y option makes the command non-interactive.

The -a option allows you to unregister a VM that is currently registered but not authenticated with KeyControl VME Vault. This option requires your KeyControl VME Vault credentials.

The -u and -p options allow you to specify a KeyControl user account name and password with Cloud Admin privileges. If you do not specify the credentials, or if you specify the user name but not the password, you will be prompted to enter this information.

rename newname

Changes the registered name of the VM with KeyControl. If there is no VM called "newname" in the Cloud VM Set to which this VM belongs, the registered name of the VM will be changed to "newname".

KeyControl Management

updatekc kc_hostname[:port],kc_hostname2[:port2],...

Manually updates the list of KeyControl node IP addresses on the VM. Having the correct list of IP addresses enables automatic failover in case one of the nodes becomes unreachable.

kc_hostname is a comma-separated list of KeyControl cluster nodes and, optionally, port numbers. The default port is 443. To enable failover, you should enter the IP address of every KeyControl node in the cluster. For example, if you have a three node cluster, you would enter

192.168.162.133,192.168.162.135,192.168.162.137.

Note that if you add or remove any nodes, you should run the "hcl updatekc" command to replace this list. Alternatively, if you have set up a KeyControl mapping, you can enter a single IP address and then select a KeyControl mapping when prompted.

updatekc -a [-n mapping] [-u username [-s password]]

Queries KeyControl for the available KeyControl mappings and allows you to select the mapping you want to use on this VM. This allows you to change to a new mapping. This command requires KeyControl Cloud Admin credentials.

The Cloud Admin can maintain multiple KeyControl mappings in KeyControl. Each of these mappings is a list of KeyControl nodes. You can associate the VM with one of those mappings. If you do, the list of KeyControl nodes will be fetched from the KeyControl and updated automatically during each heartbeat.

You will be prompted to enter your Cloud Admin credentials to use this command.

The -n option allows you to specify a KeyControl mapping for the VM. If KeyControl has mappings available for the specified Cloud Admin, and this option is omitted, the list of mappings will be displayed and you will be prompted to select one. If you choose to associate the VM with a mapping, the KeyControl list will be automatically updated when the VM heartbeats against the cluster.

The -u and -s options allow you to specify a KeyControl user account name and password with Cloud Admin privileges. If you do not specify the credentials, or if you specify the user name but not the password, you will be prompted to enter this information.

Policy Agent Certificate Management

updatecert [-p certificate_password] /path/to/cert.bin

Updates the certificate on the VM using a local copy of the certificate.

Certificates are valid for one year by default unless you changed the expiration date when the certificate was created. To maintain access to data you should create a new certificate prior to expiration, copy that certificate to the VM, and use the "hcl updatecert" command to add the new certificate.

The -p option allows you to specify the passphrase for the certificate if one was specified when the certificate was created in the KeyControl webGUI. If you omit this option and a passphrase is required, you will be prompted to enter the passphrase.

updatecert -a [-u username [-p password]] [-e certificate expiration]

Updates the certificate on the VM through KeyControl.

This form of "updatecert" allows you to download the certificate automatically through KeyControl instead of manually creating the certificate in the webGUI and copying it to the VM.

The -u and -p options allow you to specify a KeyControl user account name and password with Cloud Admin privileges. If you do not specify the credentials, or if you specify the user name but not the password, you will be prompted to enter this information.

The -e option allows you to specify the certificate expiration date using the format MM/DD/YYYY. For example, 12/25/2017. If the expiration date is not specified, the certificate will be valid for one year from the date of creation.

update_ca -f /path/to/cert.pem

Updates the local certificate bundle.

In case of any updates to the SSL certificate on KeyControl cluster you should download the certificate, copy that certificate to this computer, and use the "hcl update_ca" command to apply the new certificate.

Authentication

auth [-o one_time_passphrase]

Sends an authentication request from the VM to KeyControl. After you run this command, a Cloud Admin must complete the authentication process in KeyControl. The one-time passphrase will be expired after 15 minutes.

This command is needed if a VM fails to contact to the KeyControl cluster within "grace period" seconds or if the hardware ID changes. In the latter case, this will occur if you change the IP address or a network card.

If the KeyControl cluster is in degraded mode, this command will fail with the suggestion that the user should run: "hcl auth -a [-u user [-s password]]" instead.

auth -a [-u user [-s password]]

Authenticates the VM with KeyControl in a single step by providing the KeyControl Cloud Admin credentials.

The -u and -s options allow you to specify a KeyControl user account name and password. If you do not specify the credentials, or if you specify the user name but not the password, you will be prompted to enter this information.

If the KeyControl cluster is in degraded mode, you can still authenticate the VM if the connection failure is due to grace period expiration. The authentication will fail if the hardware signature of the VM or IP address does not match the stored value on KeyControl or the VM has been revoked by the Cloud Admin.

Note that the above restrictions do not apply if the KeyControl cluster is healthy.

Disk Encryption

list [registered|available|all]

Lists the various devices on the system. If no argument is given, it prints a list of the registered devices using the following format

device mapped-device status

You can also filter the display using the "registered", "available" or "all" arguments. In this case, the output will be in CSV format. For example:

device,mapped-device,status,guid

Windows clients will produce the following output

disk,partition,drive,status,guid

encrypt [-s] [-c cipher] [-m mapped_device] [-e days_to_expire] [-z "NO USE"|"SHRED"] [-o] [-y] [-x] diskname

Encrypts a disks that already has a filesystem/data on it that you want to preserve. This can take a fair amount of time depending on the size of the device and the processor / storage you have in place. The disk will be registered with the KeyControl cluster, which allocates a unique, per-disk encryption key.

As part of the encryption process, a HyTrust GUID and private region will be added if space is available.

If the operation is interrupted, you can complete the encrypt operation by running the command again. Encryption will continue from the place where it was interrupted.

Note that if you have migrated a disk from another VM and the disk is stamped with a HyTrust GUID, you should use the "hcl import" command to add the disk.

The -s option (Linux only) tells hcl to only encrypt allocated blocks which can reduce the time to encrypt dramatically. It uses system- provided utilities to determine the allocated filesystem blocks on a device. The current release supports this option on ext2/ext3/ext4 file systems. Note that -s option does not work in the presence of "online encryption". If "htcrypt" driver is loaded, then HTDC PA makes the clear text device available, immediately. At that point the device can be mounted and accessed through the file system. As the file system can change the free block map, we can not use it to skip free blocks.

The -c option allows you to specify the encryption cipher. Run "hcl ciphers" for the list of available ciphers.

The -e option allows you to specify the number of days the key should be active before it expires. If this option is not specified, the key never expires. What happens when a key expires is determined by the -z option.

The -z option allows you to specify what happens if a key expires. If you specify "NOUSE", the key is deactivated but retained. It can then be reactivated in the KeyControl webGUI. This is the default. If you specify "SHRED", the key is destroyed and cannot be retrieved.

The -m option (Linux only) allows you to change the default clear text path, which is constructed based on the current path to the disk. For example, if the disk is /dev/sdb1, the default clear text path would be /dev/mapper/clear_sdb1. To set the clear text path to /dev/mapper/clear_disk1, you would use "-m clear_disk1".

Note: Windows retains the same drive letter and label after reformatting, so the -m option is not needed.

The -y option makes the command non-interactive.

The -x option (Windows data drive only) causes hcl to check for the existence of a pagefile on the designated drive and will abort if one is found.

Note: By default, you cannot access a whole disk. You should always used partitioned disks since we can easily identify them (through on-disk GUIDs) and find the associated keys. You can override this feature using the -o option.

This command does not apply to boot disks.

decrypt [-s] [-y] diskname

Decrypts a disk and removes it from HyTrust's control but leaves the filesystem and data intact.

The disk will be deregistered with the KeyControl cluster, which deletes the encryption key, just like the the "rm" operation.

If the operation is interrupted you can complete the "decrypt" operation by running the same command again. Decryption will continue from where it was interrupted.

The -y option makes the command non-interactive.

The -s option (Linux only) tells hcl to only decrypt allocated blocks which can reduce the decryption time dramatically. It uses system provided utilities to determine the allocated blocks on a device. The current release supports this option on ext2/ext3/ext4 file systems. Note that -s option does not work in the presence of "online decryption". If "htcrypt" driver is loaded, then HTDC PA keeps the clear text device available, even as the device is being decrypted. As the file system can change the free block map, we can not use it to skip free blocks.

This command does not apply to boot disks.

resize [-y] diskname (Linux Only)

Resizes an active Linux disk and retains any filesystem or data. Note that resize command does not work in the presence of "online encryption". Please refer the admin guide section "Disk Size Management in Linux", for more details on volume resize.

This command resizes the crypto mapping for this disk so that it matches the size of underlying device.

The -y option makes the command non-interactive.

For example, if you have an ext2/ext3/ext4 file system on device myvg-myvol (LVM volume), you can use the following sequence of operations to extend the volume and file system online:

lvextend -L<new size> /dev/myvg/myvol

hcl resize myvg-myvol

resize2fs /dev/mapper/clear_myvg-myvol

This command does not apply to boot disks.

extend drive (Windows Only)

Extends the size of an encrypted Windows partition.

The disk must first be extended using the tools available to the hypervisor. Then the "extend" command can be used to extend the disk. Any hidden metadata partitions are taken in to account. This command does not apply to Windows boot disks.

rekey [-u] [-s] diskname

Rekeys an encrypted disk with a new encryption key. This operation involves creating a new key, decrypting the disk with the old key, and re-encrypting it with the new key. You do not need to do anything through the webGUI for this operation. Note that this operation can take a long time depending on the amount of data and CPU/storage speed.

If the operation is interrupted, you can reverse the rekey by specifying the -u option. Alternatively if you run "hcl rekey" again, it will continue from where it was interrupted.

Please note that on Linux the disk is detached and the contents are unavailable during a rekey operation.

The -s option (Linux only) tells hcl to only rekey allocated filesystem blocks which can decrease the rekey time dramatically. It uses system-provided utilities to determine the allocated blocks on a device. The current release supports this option on ext2/ext3/ext4 file systems. Note that -s option does not work in the presence of "online rekey". If "htcrypt" driver is loaded, then HTDC PA keeps the clear text device available, even as the device is being rekeyed. As the file system can change the free block map, we can not use it to skip free blocks.

This command does not apply to boot disks.

rekey status diskname

It shows the state of the encryption operation on the disk while it is in progress. Although the name of the command refers to "rekey", it shows statistics for any of encrypt, decrypt and rekey operations.

add [-F fstype | "none"] [-n] [-c cipher] [-m mapped_device] [-p parent disk] [-e days_to_expire] [-z "NO USE"|"SHRED"] [-o] [-y] [-x] diskname

Registers a new disk with KeyControl and creates a new encryption key for that disk. Note: If the disk already contains a filesystem and/or data you want to retain, use the "hcl encrypt" command instead. By default, "hcl add" reformats the disk.

On Linux, only the disk name should to be specified (for example "sdb1" as opposed to "/dev/sdb1"). On Windows the disk must already have a drive letter which is then used as the diskname argument.

By default, this command checks for the presence of an existing HyTrust GUID. If it finds one, it adds the disk without reformatting. Otherwise, it formats the disk and adds a HyTrust GUID and private region. For Windows, the only supported format is NTFS. For Linux, the default format is ext3.

The -F option (Linux only) allows you to specify a format other than ext3. You can also use -F to specify that the disk should not be formatted by specifying "-F none".

The -n option allows you to specify that the disk should not be attached immediately. You can use this option if you want to prepare the disk but not bring it online until later.

The -c option allows you to specify the encryption cipher. Run "hcl ciphers" for the list of available ciphers.

The -m option (Linux only) allows you to change the default clear text path, which is constructed based on the current path to the disk. For example, if the disk is /dev/sdb1, the default clear text path would be /dev/mapper/clear_sdb1. To set the clear text path to /dev/mapper/clear_disk1, you would use "-m clear_disk1".

Note: Windows retains the same drive letter and label after reformatting, so the -m option is not needed.

The -p option allows you to specify a snapshot of the encrypted LVM volume by specifying the name of the registered parent volume. To get the exact name, run "hcl status".

WARNING: If the snapshot was taken before registering the parent volume, then the snapshot will not have encrypted data.

The -e option allows you to specify the number of days the key should be active before it expires. (If this option is not specified, the key never expires.) What happens when a key expires is determined by the -z option.

The -z option allows you to specify what happens if a key expires. If you specify "NOUSE", the key is deactivated but retained. It can then be reactivated in the KeyControl webGUI. This is the default. If you specify "SHRED", the key is destroyed and cannot be retrieved.

By default we will prevent you from accessing a whole disk. You should always used partitioned disks since we can easily identify them (through on-disk GUIDs) and find the associated keys. You can override this by passing the -o option.

The -y option makes the command non-interactive.

The -x option (Windows data drive only) tells hcl to check for the existence of a pagefile on the designated drive and will abort if one is found.

import [-y] [-w] [-n] [-m mapped_device] [-c cipher] diskname

Add a device that has been copied/moved from another VM. The operation requires that the device was previously registered and contains a HyTrust GUID. If no GUID is present, the operation will fail and the disk will not be modified in any way.

To see GUIDs associated with a given disk, use the "hcl status -g" command on Linux and the "hcl status" command on Windows.

A device can also be imported using its SCSI WWN (Linux only), if it does not have a HyTrust GUID. Use command "hcl status -G" to see the GUIDs/WWN

If -w option is specified, import command falls back to SCSI WWN if HyTrust GUID is not found. Note that if HyTrust GUID is present then it is used even if -w is specified.

The -y option makes the command non-interactive.

The -n option allows you to specify that the disk should not be attached immediately. The "auto_attach" property is set to "DISABLED". You can use this option if you want to prepare the disk but not bring it online until later.

The -m option (Linux only) allows you to change the default clear text path, which is constructed based on the current path to the disk. For example, if the disk is /dev/sdb1, the default clear text path would be /dev/mapper/clear_sdb1. To set the clear text path to /dev/mapper/clear_disk1, you would use "-m clear_disk1".

The -c option allows you to specify the encryption cipher that was used during the initial encryption. Run "hcl ciphers" for the list of available ciphers.

rm [-y] <diskname | -a>

Removes a single disk or all disks from HyTrust control. This issues an implicit "detach" command before removing the disk from HyTrust's configuration.

WARNING: Removing a disk will result in any data encrypted on that disk being lost. If you want to retain the data, use the "hcl decrypt" command.

You can specify a single disk name or use the -a option to remove all disks.

"hcl rm" unregisters the device from the KeyControl cluster configuration and destroys the encryption key.

The -y option makes the command non-interactive.

attach [-l [-p passphrase]] <diskname | -a>

Fetches the key associated with the encrypted device from the KeyControl cluster, "unlocks" the disk making the clear text data available via the clear text device path, and runs the attach handler, which typically mounts the device. By default, devices have the "auto_attach" property set to "ENABLED", so the attach operation is done automatically at boot time.

However, there may be cases when it is not desirable for the encrypted device to be automatically attached and exposed throughout the uptime of the machine. In such cases, the "auto_attach" property of the device should be set to "DISABLED" and attach/detach should be invoked manually.

If a disk becomes detached, for example if the VM reboots and the KeyControl cluster is unreachable, use this command to manually attach one or all disks.

The -l option allows tells the command to look for a cached copy of the keys, while the -p option allows you to specify the password that decrypts the keys and allows access to the disk. If you specify -l but do not specify -p, the command prompts you for the password. (For information about caching keys, see the "hcl cache" command.)

You can specify a single disk name or use the -a option to attach all disks.

detach <diskname | -a>

Detaches a specific disk or all disks. When a disk is detached, the filesystem will be unmounted and access to data will not be available until the disk is attached again.

The detach operation runs the detach handler associated with the device, which typically unmounts the filesystem and removes the clear text device path. The key will be removed from the VM (unless it has been cached using "hcl cache", in which case it is stored encrypted by a passphrase), encrypted data is no longer accessible until a subsequent "attach" operation fetches the key from the KeyControl cluster.

You can specify a single disk or use the -a option to detach all disks.

keyversion <diskname>

Returns current keyversion for <diskname> and if Single Encryption Key is enabled for CVMset that VM is registered to will return the latest SEK keyversion.

set property=value <diskname | -a>

Sets a property value for a specific disk or for all disks. You can specify one of the following properties:

1. mntpt=<path> If set, this property is supplied to the attach handler, a script which is run at the time of attaching a device. The default attach handler uses this value as the mountpoint of the device.

2. mntopts=<string> If set, this property is supplied to the attach handler. The default attach handler uses this value as a command line argument to the mount command. An example could be "-o rw,data=journal,commit=20".

3. auto_attach=ENABLED|DISABLED. Enables or disables auto attach. Enabling this property means that HyTrust attempts to attach the disk as soon as the system is booted or the disk will be attempted to be attached as soon as the system is booted, or whenever the KeyControl cluster is reachable. The default is "ENABLED" if not supplied.

4. attach_handler=DEFAULT|<path>. Sets the attach handler, which is a script run just after the attach operation is successful. Attach handlers are called with 2-4 arguments: e.g. default.attach <path of clear text device> <path of encrypted device> [<mountpoint>] [<mount options>] The default attach handler fscks and mounts the device if the "mntpt" property is set. The handler can be customized by modifying a copy of the default handler located in /opt/hcs/handlers/default.attach. Customized attach handlers can be used for preparing and starting applications associated with this device.

5. detach_handler=DEFAULT|<path>. Sets the detach handler, which is run just before the device is detached. Detach handlers are called with 2 arguments: e.g. default.detach <path of clear text device> <path of encrypted device>. The default detach handler attempts to "kill -9" all processes using the mount point, if any, associated with this device, unmounts the filesystem. Just like the attach handler, a customized detach handler can be used to shutdown applications and carry out cleanup activities and unmount the filesystem before the device is detached. Note that a detach handler must succeed.

You can specify a single disk name or use the -a option to set the property value for all disks.

Disk Management

devorder print

Displays the current device order. To change the order, use the "devorder" command, described below.

Devices are attached automatically at boot in the order in which they were initially registered. On Linux, if the "mntpt" property is set on the device then it is also automatically mounted when attached. So the devices are mounted in the order in which they are initially registered.

This order can be changed using "devorder" command. The "devorder print" command shows the current device order.

devorder <up | down> diskname

Changes where the specified device falls in the device attach order.

The "up" option moves the device higher in the order.

The "down" option moves the device lower in the order.

updateconfig

Updates the HyTrust config file on a VM when devices have been removed or added, while the VM is online. This command lets you update the device list in "real time" without needing to reboot the VM. You do not need to run this command to update the devices that were removed or added while the VM was offline, as those updates happen automatically when the VM boots.

devicesync [-y] reason_for_sync

Synchronizes the registered device list on KeyControl with the HyTrust config file on the VM. It is particularly useful when KeyControl and the VM go out of sync after the VM is restored to an older snapshot.

As this causes a major configuration change, the admin must provide a "reason" for running this command. The information provided by admin, which should be a simple text string which is then logged in the audit log on KeyControl and added to the alert message generated during sync processing.

The -y option makes the command non-interactive.

We recommended that the admin runs the "hcl updateconfig" command after "hcl devicesync".

gone <list | rm | test> [device]

The gone command can be used to manage the hidden devices that have been marked "GONE" in the hcl config file. Devices are marked GONE when, during initial device discovery, a device which was previously encrypted is found missing. The device is not automatically deleted in order allow for recovery of accidentally removed devices.

gone list produces a list of all devices marked "GONE" in the config file. It will print both the device name and it mapped name.

gone rm device removes the hidden "GONE" entry in the config file. On the next heartbeat, it will also remove the associated entry from the KC.

gone test device returns 1 (TRUE) if the hidden device entry is marked "GONE" and 0 (FALSE) if it is not.

The device name used by both the rm and the test command can either be the physical device name or its current mapped name. These are presented in the hcl gone list command.

Disk Key Caching

cache [-n duration in days] [-p passphrase] <diskname | -a>

Caches the encryption keys for a specific disk or all disks locally on the VM for the specified number of days.

Encryption keys are generally fetched from the KeyControl cluster when a disk is added or post boot/ authentication. If you have an unstable network connection between the VM and the KeyControl cluster or you are using the DataControl agent on a VM that is not always connected to the network, you can cache the keys on the VM.

The -n option allows you to specify the number of days that the keys should be kept in the cache. Once this time expires, the keys are deleted. If the -n option is not specified, keys will be cached for a default of one day.

The -p option allows you to specify a password that must be supplied to encrypt/decrypt the keys in the cache.

You can specify a single disk name or use the -a option to cache the keys for all disks.

cache -l

Displays information about disks for which keys have been cached and the duration for which the cached keys are valid.

cache -r <diskname | -a>

Removes cached keys for a specified disk or for all disks.

You can specify a single disk name or use the -a option to remove the cached keys for all disks.

File Encryption

keyid <-c keyid_to_create [-s] [-a cipher] [-d description] [-e days_to_expire] [-k key] [-i initialization_vector] [-o "NO USE"|"SHRED"]>

Creates a KeyID, which is a handle for an encryption key that is shared between VMs in the same Cloud VM Set. KeyIDs can be used to encrypt and decrypt files which can be either passed securely between these VMs or placed on external storage for backup. For example, you can encrypt an archive from a VM that has the Policy Agent installed and move that encrypted image safely to cloud storage.

The -c option allows you to specify the name of the new KeyID.

The -s option tells KeyControl to make sure the cipher specified with the -a option is compatible with the version of OpenSSL currently installed on the VM.

The -a option allows you to specify the encryption cipher. Run "hcl ciphers" for the list of available ciphers.

The -d option allows you to specify a description for the KeyID. We recommend you use this option to better identify KeyIDs.

The -e option allows you to specify the number of days the KeyID should be active before it expires. (If this option is not specified, the KeyID never expires.) What happens when a KeyID expires is determined by the -o option.

The -k option allows you to specify the base64 encoded key string for the keyID to be created. The key value should have proper length corresponding to the cipher algorithm chosen.

The -i option allows you to specify the base64 encoded initialization_vector(IV) for the keyID to be created, the Initialization_vector must be present when using the -k option and the length must be at least 16 bytes(128 bits).

The -o option allows you to specify what happens if a KeyID expires. If you specify "NOUSE", the key is deactivated but retained. It can then be reactivated in the KeyControl webGUI. This is the default. If you specify "SHRED", the KeyID is destroyed and cannot be retrieved.

keyid -r [-f]

Removes the specified KeyID. Without the -f option, you will be prompted to confirm the removal of the KeyID.

keyid -F <keyid to fetch>

Retrieves the base64 encoded value of the key and IV associated with the keyid.

keyid -u [-d description]

Updates the specified KeyID. Currently the only attribute that can be updated is the description for the KeyID, which you specify with the -d option.

keyid -l

Displays a list of KeyIDs available to the VM based on the Cloud VM Set with which this VM is registered. You can also view the list of KeyIDs in the KeyControl webGUI.

encryptfile [-k keyid] filename [encryptedfile]

Encrypts the specified file.
The -k option allows you to specify an existing keyID to use for the encryption.
The "encryptedfile" option allows you specify a file name into which the encrypted output will be placed. By default, the command writes the output to stdout.

decryptfile encryptedfile [filename]

Decrypts a file encrypted with the "encryptfile" command on this VM or on any other VM in the Cloud VM Set.
When a file is encrypted using the "encryptfile" command, information about the keyID is stored in the encrypted file. From the same VM or any other VM in the same Cloud VM Set, you can decrypt the file using the "decryptfile" command.
The "encryptedfile" option allows you to specify the name of the file that you want to decrypt.
The "filename" option allows you specify a file name into which the decrypted output will be placed. By default, the command writes the output to stdout.

Clone Handling

template <-i ipaddr | -m macaddr> [-u username -p password] days_to_expire

This command prepares a VM for automatic clone deployment. The VM on which we run this command is called the template VM. The IP address or the MAC address can be specified with the -i or -m option respectively. The IP address or the MAC address for the clone VM must be known in advance.
Running the "hcl template" command on a template VM has two effects. First, KeyControl will recognize a VM with the provided IP or MAC address and the same certificate as a legitimate clone. Secondly, KeyControl provides limited access to keys. The "hcl template" command downloads a token which is later used to automatically register the clone VM.
The "days_to_expire" option specifies the number of days for which the clone access token remains valid.
The -u and -p options allow you to specify a KeyControl user account name and password with Cloud Admin privileges. If you do not specify the credentials, or if you specify the user name but not the password, you will be prompted to enter this information.
The sequence of operations in which this command is used is:
1. Install the Policy Agent software on the template VM.

2. Register the template VM with KeyControl.

3. Encrypt the required data devices (root device, swap etc).

4. Reserve IP addresses or MAC addresses for the clone VMs.

5. Run the "hcl template" command on the template VM.

6. Take a clone of the template VM using hypervisor tools.

7. When the clone VM boots, it will be automatically deployed and registered with a new name on KeyControl.

template remove <-i ipaddr | -m macaddr> [-u username -p password]

Removes the previously added IP address or MAC address as a legitimate clone of this VM

template list

Displays a list of all IP addresses and MAC addresses which have been added as legitimate clone VMs of this VM.

Miscellaneous

heartbeat

This command sends a heartbeat message to the KeyControl immediately instead of waiting for the hcld deamon to do it periodically. Upon successful completion, the "Last Heartbeat" field will be updated to indicate how long it has been since the client and the KeyControl have successfully communicated and the return code will be 0. If an error occurs, it will return the errno. This command can be useful to test connectivity between the VM and KeyControl.

You can view the "Last Heartbeat" field using the "hcl status" command.

ciphers

Displays the default and available ciphers.

aesni-check

Checks the CPU features to see if AES-NI crypto acceleration is available to the VM on which it is running.

htcrypt-check

Checks if the htcrypt encryption driver is present and usable.

destroy [-y]

Removes all HyTrust configuration about all disks and folders from the VM. This has the same effect as uninstalling and re-installing the product and should be used with extreme caution. This operation cannot be reverted and all encrypted data will be lost. Note that any cleanup on the KeyControl must be performed separately.

When dealing with VM clones, Do Not use this command unless VM is registered as a clone (refer 'hcl register') to avoid any accidental data loss.

To completely remove the VM from the KeyControl, the 'hcl unregister' command should be issued prior to the 'hcl destroy' command.

The -y option makes the command non-interactive.

version

Displays the version of the DataControl Policy Agent software.

-h | -?

Displays all the options available through the hcl command.

FILES

On Linux:

/opt/hcs

The default location of the Policy Agent configuration files.

/var/log/hcl.log

The Policy Agent log file. If errors are detected, you will be requested to provide this file to HyTrust support staff.

On Windows:

C:\Program Files\hcs\hcl.log

The Policy Agent log file. If errors are detected, you will be requested to provide this file to HyTrust support staff.

BUGS

See the HyTrust Release Notes for information about bugs and caveats in the software.

AUTHOR

HyTrust Inc.

SEE ALSO

htroot(1)

htroot Man Page

NAME

htroot - Encrypt Linux Root devices using HyTrust DataControl

SYNOPSIS

htroot [OPTIONS]

DESCRIPTION

The htroot command is used to manage encrypted root disk, swap and other system devices using HyTrust's DataControl. The policy agent can be used to encrypt root disk mounted on "/", multiple swap devices and devices mounted on Linux system mount points such as "/usr", "/opt", "/home" etc. This document refers to all these devices as "Linux root devices".

OPTIONS

The options are as follows:

status

Display information about encryption status of Linux root devices.

setup [-c params.conf]

Prepare system for root device encryption. This command makes necessary modifications to grub and HyTrust configuration. It also installs required packages from external repositories, if required. The user is prompted before packages are installed.

The setup command also rebuilds initrd with additional binaries and configuration files required to encrypt the root devices.

Root disk encryption on Linux requires a separate /boot partition. If the VM does not have a separate /boot, setup fails. Please refer to the Admin Guide for more information on how to seperate the boot partition on an exsting VM.

htroot setup is an interactive process. In the preparation phase, the user is prompted to make various choices. For example the user is asked to choose appropriate network configuration.

During the preparation phase, the administrator can setup a "debug console" which can be used to monitor encryption progress. As the root device encryption happens during system boot, regular admin login does not work. Other than "debug console", the progress can also be monitored on the Virtual Machine Console.

The setup command prompts the user to enable the debug console and download ssh identity file. During the root device encryption, the administrator can connect to debug console with this identity file, like

ssh -i <identity file> root@vm

The debug console provides various options in addition to showing the encryption progress, for example network restart, authentication with KeyControl etc.

-c option can be used to provide encryption related parameters using a config file. A sample configuration file is provided at /opt/hcs/bin/params.conf This option is useful in automating the invocation of htroot setup.

update [-c params.conf]

This command allows the user to update the grub configuration files and initrd for a previously root encrypted system. Note that even if the root device is decrypted later, the HyTrust changes to boot loader remain with the system, unless they are explicitly removed with cleanup command or the HyTrust agent software is uninstalled.

The update command is useful after a system kernel upgrade or HyTrust software upgrade. If the HyTrust software is upgraded on a system, it automatically updates the grub configuration and initrd. However if any of the encrypted Linux root device has in-progress encryption activity, at the time of HTDC upgrade then htroot update has to be done manually, after the encryption activity is over.

The update command also allows the administrator to update the network configuration used for root device encryption.

-c option can be used to provide encryption related parameters using a config file. A sample configuration file is provided at /opt/hcs/bin/params.conf This option is useful in automating the invocation of htroot update.

cleanup [-f]

The HyTrust changes to boot loader (grub), fstab, initrd can be removed with this command. If the root device is still encrypted then cleanup fails with a message that the administrator needs to decrypt the root device first.

If HyTrust agent has not made any changes to boot loader then cleanup returns immediately reporting that cleanup is not needed. However the administrator can force a cleanup with -f option.

If the cleanup command is interrupted by a user signal or system reboot then the administrator needs to run cleanup again, before running any other command.

encrypt [device list] [--noreboot] [--yes]

Prepare Linux root devices for encryption. This command makes necessary modifications in grub config and fstab, to initiate encryption in the next system boot.

device list is an optional parameter. The user can provide a comma (,) separated list of device names, which should be encrypted. The valid device names can be found in the output of command hcl status under the first column Disk name. If device list is provided htroot command checks for the validity of the operation on every device in the list. If the operation is not valid for any device in the list, for example encrypt is called on a device which is already encrypted, then the command fails.

If the device list is not provided then htroot encrypt becomes an interactive process. The user is prompted to choose root device, swap devices and other mount points to be encrypted under root device encryption. In the interactive mode the user can choose to encrypt root device, any or all of the swap devices and additional system mount points like /var, /usr, /opt if they are mounted on separate block devices.

Please note that in interactive mode the admin needs to provide "Mount Points" for /var, /usr, /opt etc. and not the disk or partition name. Whereas in non-interactive mode all devices are specified using "Disk Names".

Note that for root device encryption, the block device should have an entry in /etc/fstab.

The admin can run htroot encrypt multiple times and choose any of the system devices in any order. All the prepared devices will be encrypted during the next boot.

At the end of the preparation phase, htroot prompts the user to reboot the system. During subsequent boot the selected devices are encrypted. The progress of encryption can be seen on the VM console and debug console.

If --noreboot option is specified then the system will not be rebooted after the operation. The admin will have to manually reboot the system to initiate the encryption.

--yes option can be used to take affirmative action for all the confirmations.

decrypt <device list | -a> [--noreboot] [--yes]

Prepare the Virtual Machine for decryption of Linux root devices. At the end of this command the user is prompted to reboot the system.

device list is an optional parameter. The user can provide a comma (,) separated list of device names, which should be decrypted. The valid device names can be found in the output of command hcl status under the first column Disk name. If device list is provided htroot command checks for the validity of the operation on every device in the list. If the operation is not valid for any device in the list, for example decrypt is called on a device which is not encrypted, then the command fails.

The admin can specify -a instead of device list. If -a is specified then all the encrypted Linux root devices are decrypted.

If --noreboot option is specified then the system will not be rebooted after the operation. The admin will have to manually reboot the system to initiate the decryption.

--yes option can be used to take affirmative action for all the confirmations.

rekey <device list | -a> [--noreboot] [--yes]

Prepare the Virtual Machine for Linux root device rekey. At the end of this command the user is prompted to reboot the system.

device list is an optional parameter. The user can provide a comma (,) separated list of device names, which should be rekeyed. The valid device names can be found in the output of command hcl status under the first column Disk name. If device list is provided htroot command checks for the validity of the operation on every device in the list. If the operation is not valid for any device in the list, for example rekey is called on a device which is not encrypted, then the command fails.

The admin can specify -a instead of device list. If -a is specified then all the encrypted Linux root devices are rekeyed.

If --noreboot option is specified then the system will not be rebooted after the operation. The admin will have to manually reboot the system to initiate the rekey.

--yes option can be used to take affirmative action for all the confirmations.

version

Display the version of the DataControl agent software.

-h | -?

This command displays all the options available through the htroot command.

FILES

/opt/hcs

The default location of the HyTrust DataControl configuration files.

/var/log/htroot.log

The HyTrust DataControl htroot log file. If errors are detected, you will be requested to provide this file to HyTrust support staff.

/opt/hcs/bin/params.conf

Sample configuration file for supplying parameters to htroot

BUGS

See the HyTrust Release Notes for information about bugs and caveats in the software.

AUTHOR

HyTrust Inc.

SEE ALSO

hcl(1)

hcs3 Man Page

NAME

hcs3 - Encrypted files on Amazon S3 using HyTrust DataControl

SYNOPSIS

hcs3 [OPTIONS]

DESCRIPTION

The hcs3 command is used to manage encrypted files on Amazon S3 using HyTrust's DataControl.

OPTIONS

The options are as follows:

status

Display information about stores, buckets and properties.

setstore aws_access_key_id aws_secret_access_key

Cache the AWS access key and secret key in local configuration file. The policy agent keeps the credentials in an encrypted configuration file.

To clear the previously set values, run setstore with empty strings, like

hcs3 setstore "" ""

Alternatively the user can also use environment variables to pass the AWS credentials to hcs3 commands. Following variables are required -

AWS_ACCESS_KEY_ID - AWS access key. AWS_SECRET_ACCESS_KEY - AWS secret key.

Access and secret key variables override credentials stored in credential and config files.

useraccess <-d | -e no_of_days>

hcs3 command can only be used by root user or Administrator (Windows) by default.

Enable the access for non-root (non-Administrator) user. The access can be enabled for specific number of days (-e). If the zero number of days are specified, then the access is enabled for ever until specifically revoked using "-d" option.

The root user can disable the non-root access using -d option.

create bucketname

This command creates a bucket in AWS S3. It also creates a default key for encrypting the files which are uploaded to this bucket. Note that the actual bucket name in Amazon S3 might differ.

delete bucketname

This command removes the specified bucket in S3. It also removes the default encryption key for this bucket. Note that if the bucket is not empty, then it can not be removed.

set property=value

There is only one property supported at present. "tmp" can be set to full path of any directory to which the user has access. This directory is used to temporarily hold the files as they are encrypted or decrypted, in transit.

To clear the previously set property, run set with empty strings, like

hcs3 set tmp=

list [bucketname]

This command displays all the buckets accessible with the current AWS credentials. If the bucketname is specified then it displays the list of files in the given bucket.

add [-k keyid] [-s] bucketname filename

Add a file "filename" to AWS S3 bucket. The file is encrypted with the default key for this bucket. "filename" can be relative or absolute pathname. The filename specified here is used as identifier for the file in the AWS bucket.

If -k keyid is specified then this key is used to encrypt the file instead of the default key.

If -s is specified then the command shows upload statistics as the file is copied to AWS.

rm bucketname filename

This command removes the specified file from the bucket identified by "bucketname".

get [-s] bucketname filename [ofilename]

This command retrieves the specified file from AWS bucket. The decrypted file is copied to the location specified by "filename"

If "ofilename" is specified then the decrypted file is copied to this path.

If -s is specified then the command shows download statistics as the file is copied from AWS.

version

Display the version of the DataControl agent software.

-h | -?

This command displays all the options available through the hcs3 command.

FILES

/opt/hcs

The default location of the HyTrust DataControl configuration files.

/var/log/hcl.log

The HyTrust DataControl log file, hcs3 logs errors here. If errors are detected, you will be requested to provide this file to HyTrust support staff.

$HOME/hcs3.log

The HyTrust DataControl hcs3 log file, when hcs3 is run as a non-root user, hcs3 logs errors here. If errors are detected, you will be requested to provide this file to HyTrust support staff. This file is created in the HOME directory of the user.

BUGS

See the HyTrust Release Notes for information about bugs and caveats in the software.

AUTHOR

HyTrust Inc.

SEE ALSO

hcl(1)

16 CSP Vault with VSAN and VMware vSphere VM Encryption

The following topics explain how to set up a CSP Vault KMIP server as a vSphere KMS (Key Management Server), which allows CSP Vault to manage the encryption keys for virtual machines that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware VSAN Encryption.

CSP Vault with VSAN and VMware vSphere VM Encryption Overview

Entrust Cryptographic Security Platform Vault supports a fully functional KMIP (Key Management Interoperability Protocol) server that can serve as a vSphere KMS (Key Management Server).

Once a trusted connection between Cryptographic Security Platform Vault and vSphere has been established, Cryptographic Security Platform Vault can manage the encryption keys for virtual machines in the cluster that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware VSAN Encryption. The procedure is identical no matter which VMware encryption method you use.

> Note: If you are using KMIP with Key Encryption Key (KEK) enabled, please ensure that the KEK cache timeout is enabled. Set the value to anything other than 0. For details, see KEKs with KMIP.

To set up Cryptographic Security Platform Vault as a KMS for vSphere:

Step	Task	Notes
1	If you currently have a different KMS configured in vCenter that you want to replace with Cryptographic Security Platform Vault, make sure you decrypt all workloads associated with that KMS and that you remove the KMS from vCenter. You can then set up Cryptographic Security Platform Vault as your KMS.	For details on decrypting workloads or removing a KMS from vCenter, see your vCenter documentation.
2	Have access to a Cryptographic Security Platform Vault cluster that has been properly configured and is operational. Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.	For details, see Installation Overview.
3	Configure a KMIP server in the Cryptographic Security Platform Vault cluster.	See Configuring a KMIP Server for vSphere KMS.

Step	Task	Notes
4	Add a KMS Cluster in vSphere using the VMware vCenter Web Client. Important: Do *not* enter a user name or password for the KMS cluster.	See Adding a KMS Cluster in vSphere.
5	Establish a trusted connection to the Cryptographic Security Platform Vault KMIP server by creating a client certificate bundle on the KMIP server and uploading it to vSphere. You can create the KMIP client certificate bundle using a Certificate Signing Request (CSR) generated by vSphere or generated by Cryptographic Security Platform Vault. Important: Do *not* enter a password for the certificates. Due to a vSphere limitation, you cannot upload encrypted certificates.	See Establishing a Trusted Connection with a CSP Vault-Generated CSR.

Configuring a KMIP Server for vSphere KMS

After your Cryptographic Security Platform Vault cluster is configured, you need to enable the included KMIP server. This server becomes the vSphere KMS (Key Management Server) when you establish a trusted connection between vSphere and Cryptographic Security Platform Vault.

If you have already enabled the KMIP server in the cluster, make sure the configuration settings match the ones given below.

For details about the Entrust KMIP server implementation and how to manage KMIP server objects, or how to configure KMIP with a Hardware Security Module (HSM), see KMIP Server Configuration or Hardware Security Modules with CSP Vault.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

1. Log into the Cryptographic Security Platform Vault Management webGUI.
2. Select the Settings icon at the top right of the vault page.
3. On the KMIP Vault Settings page, complete the following:

Option	Description
State	If set to Enabled, clients can connect to this KMIP server.
Port	The server port number. The default port is 5696.
Verify	If set to Yes, the KMIP client identity is verified before the server handles its request. We recommend that you do not turn this option off.

Option	Description
Log Level	The lowest level of log messages that will be saved in the audit log. The options are: • **All**—Logs all requests to the KMIP server and responses from the KMIP server. • **Create-Modify**—Logs object creation, object modify requests, and object delete requests and responses. This is the default. • **Create-Get**—Logs object creation messages, object fetch requests, and object fetch responses. • **Create**—Logs object creation request and response messages. • **Get**—Logs object fetch and object locate requests and responses. • **Off**—No log messages are stored in the audit log.
TLS	Choose which version of TLS you want to support. If set to TLS 1.3, all clients must connect to this KMIP server using TLS 1.3. By default, both TLS 1.2 and TLS 1.3 are supported. Note: The TLS setting applies to the KMIP server only and affects the entire cluster.
Timeout	The length of time, in minutes, after which a client request will time out. If No is selected, client requests never time out. This is the default. To change this option, select Yes and select the number of minutes before the requests times out. This can be from 1 to 60 minutes.

Option	Description
KMIP Locate Operation: Maximum Items Default	Choose the maximum number of items to be returned from the KMIP server `Locate` operation. Note: The KMIP client allows you to set an offset items value (the record number the return starts with) and a maximum items value (how many items are returned) when you run the KMIP locate operation. The maximum number of items depends on both the choice that you set in the webGUI and the value that you set in the KMIP Client. For example: • If you choose the default value in the webGUI, and you DO set a max value in the KMIP Client, it returns up to 1000 UUIDs. • If you choose the default value in the webGUI, and you do NOT set a max value in the KMIP Client, it returns up to 100 UUIDs. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you DO set a max value, it returns the maximum value of UUIDs that is set in the KMIP Client. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you do NOT set max value, it returns all the UUIDs found in the locate operation. For more information on the KMIP `Locate` command, see https://docs.oasis-open.org/kmip/kmip-spec/.
SSL/TLS Ciphers	Enter the SSL ciphers in a comma-separated list that you want the KMIP server to use. Note: The following ciphers are not supported: DHE-DSS-AES128-256 and DHE-DSS-AES128-SHA256.

Option	Description
Certificate Types	This can be one of the following: If set to Default, the KMIP server uses a default certificate. If set to Custom, you must have a custom SSL certificate generated from Cryptographic Security Platform Vault or from your own CSR, and then provide the following: • SSL Certificate—Upload the SSL certificate file in Base64-encoded pem format. It should be able to function as a server certificate. • CA Certificate—Upload the certificate for the CA that signed the custom SSL certificate in Base64-encoded pem format. If you want to use the CA certificate to verify the KMIP client certificate select **Yes**. The default is **No**. **Important:** If you select Yes, you will need to upload a KMIP client certificate for every Cryptographic Security Platform Vault for KMIP. • Private Key—Optionally upload the private key file in Base64-encoded pem format. This is required if you used your own CSR and not the CSR generated on the KMIP page. • Password—Optionally enter the password for the custom certificate.

4. Click **Apply** and confirm your changes when prompted.

What to Do Next

Create the KMS cluster in vSphere as described in Adding a KMS Cluster in vSphere.

Adding a KMS Cluster in vSphere

1. Launch the vSphere Client and log into the vCenter server that you want to add to Entrust Cryptographic Security Platform Vault.
2. Select the vCenter Server in the Global Inventory Lists.
3. Click **Configure**.
4. Select **Key Management Servers**.
5. Click **Add KMS** and set the following configuration options:

Option	Description
KMS cluster	Select <Create new cluster>.
Cluster name and Server alias	Enter a name and alias for the cluster. These names are local to vSphere and are not used by Cryptographic Security Platform Vault.

Option	Description
Server address	The IP address for the Entrust KMIP server. This IP address must match the Cryptographic Security Platform Vault KMIP server Host Name shown in the Cryptographic Security Platform Vault webGUI. Important: Make sure that the KMIP server resides on a device that is *not* encrypted. The KMIP server must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.
Server port	The port number for the Entrust KMIP server. The KMIP standard port is 5696.
Proxy address and Proxy port	Enter this information if required by your network administrator.
User name and Password.	Optional: The user name or password for the KMS cluster.

6. Click **OK**.
7. When prompted, click **Yes** to make this the default KMS cluster.
8. In the Trust Certificate dialog box, click **Trust**.
   Note: This adds the KMS cluster to vCenter but the connection status will be "Cannot establish trust connection".

What to Do Next

Establish a trusted connection between the KMS cluster and the Entrust KMIP server. How you do this depends on whether you want vSphere or CSP Vault to generate the Certificate Signing Request (CSR) used to establish the trusted connection. For more information, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.

Establishing a Trusted Connection with a vSphere-Generated CSR

The following procedure describes how to generate a Certificate Signing Request (CSR) in vCenter and then use that CSR to create a certificate bundle on the Entrust KMIP server. The KMIP certificate can then be uploaded to vSphere to establish a trusted connection between vCenter and the Entrust KMIP server.

You can also establish a trusted connection using a Cryptographic Security Platform Vault-generated CSR. For details, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.

1. Use the following VMware documentation to configure the KMS cluster:
   Add a Standard Key Provider Using the vSphere Client
2. Use the following VMware documentation to establish Trust:
   Establish a Standard Key Provider Trusted Connection by Exchanging Certificates
   Note: Ensure that you select the option "New Certificate Signing Request". Continue to follow the VMware procedures until you reach the point where it says "Follow the instructions from your KMS vendor to submit the CSR".
3. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
4. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**.
5. On the Client Certificates tab, click the **+** icon on right top corner to create new client certificate.

6. In the Create Client Certificate dialogue, specify the options you want to use and click **Create**.

Field	Description
Certificate Name	A user-defined name for this bundle. If you are going to create multiple KMIP certificate bundles, this name should be descriptive enough that you can tell the certificate bundles apart. The name can only contain letters, numbers, dashes, periods, underscores, and spaces, and cannot be changed after the bundle is created.
Certificate Expiration	The date on which the certificates in the bundle will expire. If the certificates expire, communication between the Cryptographic Security Platform Vault KMIP server and the client will be disrupted until a new certificate bundle is uploaded to the client.
Certificate Signing Request (CSR)	To use an external CSR, click Load File and upload the file that you just obtained from vSphere.
Certificate Password/ Confirm Password	If you have selected Encrypt Certificate Bundle, provide a passphrase to encrypt the certificates in the bundle. Whether the certificates need to be encrypted depends on the way your security is configured and the type of implementation you are using. Not all third-party KMIP clients can accept encrypted certificates. For example, if you are integrating Cryptographic Security Platform Vault with VMware vSphere Encryption, you *cannot* specify a certificate passphrase due to limitations with vSphere.

7. Select the certificate bundle you just created.
8. Click the Download button on right top corner to download the certificate bundle.
   The webGUI downloads `<certname_datetimestamp>.zip`, which contains a user certification/key file called `<certname>.pem` and a server certification file called `cacert.pem`.
9. Unzip the file so that you have the `<certname>.pem` file available to upload into vCenter. In the example above the certificate file would be named `KMIPvSphereCert.pem`.
10. Return to vCenter and follow the instructions in the following VMware documentation to upload the `<certname>.pem` file:
    Use the New Certificate Signing Request Option to Establish a Standard Key Provider Trusted Connection
    You do not need to do anything with the `cacert.pem` file.

After you have finished, please click the radio button (dot) to the left of the KMS cluster name and ensure that the Connection Status for each KMIP server in the cluster is Normal, and the Certificate Status for the overall KMS cluster is listed. The certificate status for the individual KMIP servers in the cluster can be ignored.

Establishing a Trusted Connection with a CSP Vault-Generated CSR

The following procedure describes how to create a certificate bundle on the Entrust KMIP server that uses a Certificate Signing Request (CSR) generated by Cryptographic Security Platform Vault. The KMIP certificate can then be uploaded to vSphere to establish a trusted connection between vSphere and the Entrust KMIP server.

You can also establish a trusted connection using a vSphere-generated CSR. For details, see Establishing a Trusted Connection with a vSphere-Generated CSR.

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**.
3. On the Client Certificates tab, click the **+** icon on right top corner to create new client certificate.
4. In the Create Client Certificate dialogue, specify the options you want to use and click **Create**.

Field	Description
Certificate Name	A user-defined name for this bundle. If you are going to create multiple KMIP certificate bundles, this name should be descriptive enough that you can tell the certificate bundles apart. The name can only contain letters, numbers, dashes, periods, underscores, and spaces, and cannot be changed after the bundle is created.
Certificate Expiration	The date on which the certificates in the bundle will expire. If the certificates expire, communication between the KMIP server and the client will be disrupted until a new certificate bundle is uploaded to the client.
Certificate Signing Request (CSR)	Not applicable. Do not upload any file.
Certificate Password/ Confirm Password	If you have selected Encrypt Certificate Bundle, provide a passphrase to encrypt the certificates in the bundle. Whether the certificates need to be encrypted depends on the way your security is configured and the type of implementation you are using. Not all third-party KMIP clients can accept encrypted certificates. For example, if you are integrating Cryptographic Security Platform Vault for KMIP with VMware vSphere Encryption, you *cannot* specify a certificate passphrase due to limitations with vSphere.

5. Select the certificate bundle you just created.
6. Click the Download button on right top corner to download the certificate bundle.
   The Cryptographic Security Platform Vault for KMIP webGUI downloads `<certname_datetimestamp>.zip`, which contains a user certification/key file called `<certname>.pem` and a server certification file called `cacert.pem`.

7. Unzip the file so that you have the `<certname>.pem` file available to upload into vCenter. In the example above the certificate file would be named `vSphereKMS.pem`.
8. Launch the vSphere Client and select the vCenter server to which you added the Cryptographic Security Platform Vault for KMIP KMS cluster.
9. Follow the instructions in the following VMware documentation to upload the `<certname>.pem` file:
   Use the Upload Certificate and Private Key Option to Establish a Standard Key Provider Trusted Connection
   You do not need to do anything with the `cacert.pem` file.

After you have finished, please click the radio button (dot) to the left of the KMS cluster name and ensure that the Connection Status for each KMIP server in the cluster is Normal, and the Certificate Status for the overall KMS cluster is listed. The certificate status for the individual KMIP servers in the cluster can be ignored.

Troubleshooting

Key Generation Error During Encryption

If vSphere Virtual Machine encryption or VMware VSAN encryption fails with the error "Cannot generate key", check the following:

- The Entrust Cryptographic Security Platform Vault appliance must be powered on and operational. To verify this, log into the appliance using the Cryptographic Security Platform Vault webGUI.
- The Entrust KMIP server must be enabled as described in Configuring a KMIP Server.
- The Cryptographic Security Platform Vault nodes must be able to communicate with one another. Make sure the server status is not shown as Degraded in the Cryptographic Security Platform Vault webGUI.
- The KMIP client certificate and private key must be valid and current. You can verify the certificate status in the Cryptographic Security Platform Vault webGUI on the KMIP Servers **Users** tab or in the vCenter Client on the **KMS** tab. For details about creating a new certificate and key, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.
- If the vCenter Client reports that the KMIP connection status is Normal (green) but encryption fails, the KMS cluster could have been added with a user name and password. To verify this:
  a. Check the Entrust Cryptographic Security Platform Vault Audit log for the message "KMIP response rate OperationFailed DENIED".
  b. If you find that message, edit the properties of the Entrust KMS cluster in the vCenter Client and remove any user name or password.
- If the Cryptographic Security Platform Vault cluster is functioning properly and the certificates are valid but the vCenter Client reports that the EntrustKMS is not connected, log into the vCenter Client and navigate to the **KMS** tab. Select the Entrust KMS, then select **All Actions > Refresh KMS certificate**.
  If that does not work, you may need to remove the KMS instance and re-add it to vCenter in order to restore the Trusted connection. Select the EntrustKMS in vSphere Client and select **All Actions > Remove KMS**. Then add the KMS back as described in Adding a KMS Cluster in vSphere.
- If you are using VM encryption and everything shows as connected but encryption still fails, use the vCenter Client to verify that encryption is enabled for the ESXi host using ***ESXi-server-name* > Configure > Security Profile > Host Encryption Mode**.
- If KMIP key creation fails when KMIP KEK is enabled, check if the audit log shows "KMIP Response: Create OperationFailed DB_GENERAL". If so, retry the create operation after enabling KEK cache timeout.
- If you are attempting to encrypt VM or vSAN storage and see errors such as "Create OperationFailed DB_GENERAL" and "Admin Key Regeneration failed" in the Cryptographic Security Platform Vault webGUI and an operation failed message with "RuntimeFault.summary" status in ESXi, check your alerts to see if your KMIP license entitlement is disabled or the license has expired.

Certificate Update Errors

If you try to update the KMS certificate for a Cryptographic Security Platform Vault KMIP Server and vSphere responds with the error message:

The "Update KMS Certificate" operation failed for the entity with the following error message.

Database temporarily unavailable or has network problems.

There may be too many certificates for the KMS Cluster in the vCenter Certificate database. Please see the following knowledge base article https://knowledge.broadcom.com/external/article/383055/expired-kms-server-certificate-will-not.html, or contact Broadcom Support for assistance with this.