Cryptographic Security Platform 1.4

Compliance Manager 10.5.4 user guide

Document issue: 1.1
Issue date: August 7, 2026

© 2026, Entrust. All rights reserved

Entrust and the hexagon design are trademarks, registered trademarks and/or service marks of Entrust Corporation in Canada and the United States and in other countries. All Entrust product names and logos are trademarks, registered trademarks and/or service marks of Entrust Corporation. All other company and product names and logos are trademarks, registered trademarks and/or service marks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS O F THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Contents

1 About this guide

This guide describes how to use the cloud-based Compliance Manager application.

Revision information

See the following table for the changes in each document issue.

Issue	Date	Section	Changes
1.1	Ago 2026	Cover	Update title
1.0	Jul 2026	All	Document release

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 Compliance Manager

Entrust Cryptographic Security Platform (CSP) Compliance Manager provides centralized visibility of an enterprise's cryptographic assets and a policy engine that allows fine-grained control of keys, secrets and certificates regardless of the locations. This allows businesses to easily establish and maintain an inventory and achieve visibility on all related information for all cryptographic assets, whether located on-premise or in cloud environments. Inventory information provides granular details on which assets are being used, and can include information about the history, ownership, environment, purpose, and whether or not the asset is used in a critical system.

4 Using the Compliance Manager webGUI

This section contains:

Understanding the Compliance Manager Dashboard

The Cryptographic Security Platform Compliance Manager Dashboard allows you to view a snapshot of your data sources, their compliance, and the percentage of completed documentation. You can filter by individual data sources or view all of them together. You can also view the total number of cryptographic assets and the type.

The following sections are visible on the dashboard page:

- **World Map**—Displays a map of the world with pins to indicate where your vaults are located.
  Click the Collections drop-down menu at the top to filter what collections you want to view.
  Click the Data Source drop-down menu at the bottom to filter what data sources you want to view.
- **Data Sources**—The data sources row displays the number of data sources, their current compliance, and their current documentation. You can click on the data sources number to go directly to the Data Sources page.
- **Total Assets**—The total assets row displays all of the cryptographic assets and what data source they belong to. You can click on the total objects number to go directly to the Cryptographic Assets page, or a data source link to view all cryptographic assets in that specific data source.
- **Risk of Cryptographic Assets (Risk Score)**—Displays the total risk score for all objects in all data sources. Each vault's overall security risk score is calculated using a weighted average that reflects the individual risk scores of the objects it contains, providing a nuanced measure of the vault's security posture. The risk score provides a quantifiable measure of the security risk associated with the vault, taking into account all the cryptographic assets it contains. You can click on the risk score percentage to go directly to the Cryptographic Assets page, filtered by that risk score.
- **Compliance Trends**—Displays trending information for your compliance policies.
- **Documentation Trends**—Displays trending information about your documentation.

Getting Started with the Compliance Manager webGUI

To start using the Cryptographic Security Platform Compliance Manager webGUI, you will need to do the following:

Step	Description	Notes
1	Connect one or more data sources to Cryptographic Security Platform Compliance Manager.	See Creating a Data Source Connection.
2	Create a collection to organize your Cryptographic Security Platform Vaults, or use the default collection.	See Creating a Collection.

After you have added a data source, you can start viewing the cryptographic assets in the vault.

Accessing the Compliance Manager webGUI

Administrators for a tenant will receive an email that gives you the URL, user name, and temporary password for Cryptographic Security Platform Compliance Manager. If email notifications are not available, then the tenant manager will need to send you the information separately.

When you access the Cryptographic Security Platform Compliance Manager webGUI for the first time, you will need to read and agree to the Entrust End User License, and then immediately change the temporary password before you can continue.

After accessing the Cryptographic Security Platform Compliance Manager webGUI, you will see a welcome page with links to adding data sources or the settings page where you can invite additional members or configure authentication.

CSP Compliance Manager Users

Cryptographic Security Platform Compliance Manager has the following users:

- Administrators—An administrator can add, edit, and view all collections.
- Auditors—An auditor has view access for all collections.

5 Collections and Data Sources

This section contains:

Managing Data Sources

Data sources are managed in the webGUI for the specific data source. For example, if you want to manage a Cryptographic Security Platform Vault for CloudKeys, you would use the Cryptographic Security Platform Vault for CloudKeys webGUI. If you want to manage an HSM in the Cryptographic Security Platform Vault, you would use the KeySafe5 webGUI for that HSM.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Data Sources**.
3. Highlight the data source that you want to manage and click **Manage**.
   The webGUI for your data source will launch in a separate window.

Disconnecting or Reconnecting a Data Source Connection

You can disconnect or reconnect a data source connection in the Cryptographic Security Platform Compliance Manager webGUI.

Disconnecting a Data Source Connection

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to disconnect and click **View Details**.
4. Highlight the data source that you want to disconnect.
5. On the far right, click the **Disconnect** icon.
6. In the Disconnect Data Source window, click **Disconnect**.

Reconnecting a Data Source Connection

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to reconnect and click **View Details**.
4. Highlight the data source that you want to reconnect.
5. On the far right, click the **Reconnect** icon.

You will be taken to the Initialize Connection to a Data Source page for the data source that you previously disconnected.
6. Click **Create and Download File**.
7. On the Data Sources page, click the **Manage** link for the data source.
   You will be taken to the data source that you want to reconnect.
8. Log in to the data source, and click the Connect Now link at the top.
   Alternatively, you can click Settings and then Cryptographic Security Platform Compliance Manager.
9. Click **Connect** and upload the file that you just downloaded.
10. Click **Close** to close the window.

Moving a Data Source to a Different Collection

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to move and click **View Details**.
4. Highlight the data source that you want to move and click the **Move** icon.
5. In the Move Data Source to Collection window, select the collection where you want to move the Data Source and click **Move**.

Viewing Connected Data Source Connections

You can only edit data source details from the Collections page. To actually make changes to the data source, see Managing Data Sources.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to edit and click **View Details**.
4. Highlight the data source that you want to edit and click the **Edit** icon.
5. In the Edit Details window, modify the following:
   - Friendly Name—How this data source is referenced in the Cryptographic Security Platform Compliance Manager.
   - Description—An optional description to describe the data source.
   - Location—The best location to represent this data source on the world map. For US locations, you can select the closest city and state. For all other locations, select the closest city.

   Note: The friendly name and the location are displayed on the dashboard.
6. When you are finished, click **Apply**.

Editing Data Source Details

You can only edit data source details from the Collections page. To actually make changes to the data source, see Managing Data Sources.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to edit and click **View Details**.
4. Highlight the data source that you want to edit and click the **Edit** icon.
5. In the Edit Details window, modify the following:
   - Friendly Name—How this data source is referenced in the Cryptographic Security Platform Compliance Manager.

- Description—An optional description to describe the data source.
- Location—The best location to represent this data source on the world map. For US locations, you can select the closest city and state. For all other locations, select the closest city.

Note: The friendly name and the location are displayed on the dashboard.

6. When you are finished, click **Apply**.

Deleting a Data Source from a Collection

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that contains the data source that you want to delete and click **View Details**.
4. On the Data Sources tab, highlight the data source that you want to delete and click the **Delete** icon.
5. In the Delete Data Source window, click **Delete**.

Creating a Data Source Connection

Initializing a connection to a data source allows the Cryptographic Security Platform Compliance Manager to import metadata from that data source.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Data Sources**.
   Note: For Cryptographic Security Platform Vault, the data sources are the individual vaults, for example, the Cryptographic Security Platform Vault for KMIP. If you want to add the Cryptographic Security Platform Vault appliance, select **Appliance Clusters** from the side menu bar.
3. Select **Actions > Initialize Connection**.
   If you do not already have a data source connected, click **Initialize Connection** on the Data Sources page.
4. On the Initialize Connection to a Data Source page, enter the URL for the data source that you want to add.
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.
6. Log into the data source that you created the connection to.
7. At the top of the page, you will see a warning that you are not connected to Cryptographic Security Platform Compliance Manager. Click **Connect Now**.
8. Click **Connect** and upload the JSON file that you downloaded from Cryptographic Security Platform Compliance Manager.
9. Click **Close** to close the Connect CSP Compliance Manager window.

Deleting a Collection

You can only delete a collection if there are no data sources in the collection, and it is not the default.

Note: The Default Collection can not be deleted.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight a collection that you have created and click **View Details**.
4. Click the **About** tab and then click **Delete Collection**.

Editing a Collection

You can edit the details of a collection and the data sources contained in that collection.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight a collection that you have created and click **View Details**.
4. Click the **Data Sources** tab, mouseover one of the data sources, and click one of the following icons:
    - Disconnect / Reconnect—See Disconnecting or Reconnecting a Data Source Connection.
    - Move—See Moving a Data Source to a Different Collection.
    - Edit—See Editing Data Source Details.
    - Delete—See Deleting a Data Source from a Collection.
5. Click the **About** tab and update the collection name or description.
6. Click **Apply**.

Creating a Collection

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Click the **Create Collection** button.
4. Enter the name of the collection. This name can be modified later.
5. Enter an optional description to help identify the collection.
6. Click **Create**.

Viewing Collections

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Collections**.
3. Highlight the collection that you want to view and click **View Details**.
    - The Data Sources tab displays all of the connected data sources in this collection. From here you can move a data source to a different collection, edit a data source, or delete an existing data source.
    - The About tab displays the collection name and description. From here you can delete a collection as long as no data sources are in the collection, and it is not the default.

About Collections and Data Sources

Data sources are organized in Cryptographic Security Platform Compliance Manager in Collections. Each collection can have one or more data sources connected to it. All data sources are added to the Default Collection when they are first connected.

Data sources include the entities that are being analyzed for compliance, including CSP Vaults (CloudKeys, Secrets, KMIP, etc.) or File Encryption. Data sources are not managed in the Compliance Manager, however, when a data source is connected, information (metadata) about the cryptographic assets within the data source is synced with the Compliance Manager every 8 hours.

6 Cryptographic Assets

This section contains:

Sending Documentation Requests

You can send an email directly to the owner of a cryptographic asset to ask them to complete the documentation.

Note: If email notifications are not enabled, then

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Cryptographic Assets**.
3. Select the cryptographic asset for which you want to send a documentation request.
4. Select the Documentation tab.
5. In the Ask Owner field, enter the email address of the owner of the cryptographic asset.

The owner of the cryptographic asset receives an email with a direct link to the documentation page for this cryptographic asset. When the owner clicks the link, they are taken directly to a Cryptographic Security Platform Compliance Manager page that does not require a login.

Note: If email is not enabled, the Ask Owner field will not be visible.

Documenting Cryptographic Assets

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Cryptographic Assets**.
3. Select the cryptographic asset that you want to document.
4. Click the documentation tab.
5. Fill in the documentation and click **Submit**.

Viewing Cryptographic Assets

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Cryptographic Assets**.
   The Cryptographic Assets page displays the cryptographic assets based upon the filters above. You can filter on collection, vault, or type of cryptographic asset as well as use the search window to narrow down your results. The columns displayed are:
   - Name—The name of the cryptographic asset.
   - Collection—The collection to which the data source belongs.
   - Data Source—The vault to which the cryptographic asset belongs.
   - Status—The status of the cryptographic asset.
   - Documented—Displays the completion percentage of the of the documentation, or No Template.
   - Compliance—Displays the compliance percentage of the cryptographic asset, or Unassessed if the cryptographic asset has not been assessed.
   - Age—Displays the age of the cryptographic asset.

- Risk—Displays the risk score for the cryptographic asset.

3. Select the cryptographic asset that you want to view. The cryptographic asset page displays the following tabs:
    - **Details**—Displays information about the cryptographic asset, such as when it was created and any the identifying information. For example:
        - Data Source—The name of the data source that the cryptographic asset belongs to.
        - Collection—The name of the Collection the cryptographic asset belongs to.
        - HSM Protected—Whether or not the cryptographic asset is protected by an HSM.
        - Dormant—Whether or not the cryptographic asset is active in a Cryptographic Security Platform Vault. When cryptographic assets are deleted, Cryptographic Security Platform Compliance Manager retains the metadata for 6 months. It takes a few days after an object is deleted in a Cryptographic Security Platform Vault to show up as Dormant.
        - Expire Action—The action, if any, to be taken when the cryptographic asset expires.
        - LastSync—The date and time that Cryptographic Security Platform Compliance Manager was last synced with the Cryptographic Security Platform Vault. The sync occurs every six hours.
        - Status—The status of the cryptographic asset.
          Note: Dormant cryptographic assets may still be listed as Active or Available if that was what the last synced metadata showed.
        - Compliance Status—Whether compliance has been run against the cryptographic asset.
        - Is Documented—Whether or not documentation has been created for the cryptographic asset.

      Note: This list is not complete.
    - **Compliance**—Displays all of the compliance runs, the score, the policy and schedule used, and the status.
    - **Documentation**—Displays the documentation template that was assigned. If there is no template, click the **View vault documentation** link to add a template.
      Whether or not there is a template, there is a Documented or Not Documented box telling you if the cryptographic asset documentation has been completed. If there is documentation, you will also see an Ask Owner box that allows you to email this page to someone who can fill out the details.

About Cryptographic Assets

All objects contained within your data sources are called cryptographic assets. For each cryptographic asset, Cryptographic Security Platform Compliance Manager tracks the following information:

- Name—The name of the cryptographic asset.
- Collection—The collection that contains the data source where the cryptographic asset is located.
- Data Source—The name of the data source that contains the cryptographic asset.
- Status—The status of the cryptographic asset. This can be one of the following:
    - Available
    - Preactive
    - Deactivated
    - Disabled
- Documented—Whether or not the cryptographic asset has documentation. This can be one of the following:
    - Documented—A documentation template has been assigned to the cryptographic asset and it is completed.
    - Not Documented—A documentation template has been assigned to the cryptographic asset, but it is not completed.
    - No Template—No documentation template has been assigned to the cryptographic asset.
- Compliance—Whether or not the cryptographic asset has been assessed by a compliance policy.
    - Compliant—The cryptographic asset has been assessed and is compliant.
    - Not Compliant—The cryptographic asset has been assessed and is not compliant.
    - Unassessed—The cryptographic asset has not been assessed.
- Age—The age of the cryptographic asset in days.

- PQ Status—If PQ Safe, the cryptographic asset is considered to be secure against a cryptographic attack by a quantum computer.
- Risk—The risk score of the cryptographic asset.

7 Reports

This section contains:

Deleting a Report

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Reports**.
3. On the Manage Reports page, you can delete reports in one of two ways:
    - On the Reports tab, locate the report that you want to delete, and click the Delete icon at the end of the row.
      This deletes the report definition which includes the schedule. The historical reports will remain on the History tab, but no more reports will be run.
    - On the History tab, locate the report version that you want to delete, and click the Delete icon at the end of the row.
      This deletes the individual version of the report, but does not delete the report definition or any other versions of the report.

Editing a Report

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Reports**.
3. On the Manage Reports page, locate the report that you want to edit, and either click the name of the report or click the Edit button at the end of the row.
4. In the Edit Report window, you can update the following information:
    - The Name of the report.
    - The Description of the report.
    - Whether or not email is enabled.
    - If email is enabled, the email addresses of the people who will receive the report.
    - The collections where the data sources are found.
    - The data sources to be included in the report.
    - How long the report history should be retained.
    - The recurring schedule for the report.
    - The frequency when the report should be run.
5. Click **Apply** to save your changes.

Creating a Report

When you create a report the report definition remains on the Reports tab. When that report is run, any versions of the report will be located on the History tab.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Reports**.
3. On the Manage Reports page, in the About section, enter the following:

Field	Description
Type	Enter the type of report you would like to create. This can be one of the following: • Executive Summary • License
Name	Enter the name for the report.
Description	Enter an optional description for the report.
Email Report To	If email is enabled, and you would like to email the report, enter the email address.

4. Click **Next**.
5. On the Manage Reports page, in the Details section, enter the following:

Field	Description
Collections	Choose the collections that you would like to include.
Data Sources	Choose the Data Sources that you would like to include.
Report Retention	Enter the amount of time you would like to keep this report.

6. Click **Next**.
7. On the Manage Reports page, in the Schedule section, enter the following:

Field	Description
Recurring Schedule	Choose Active to set a recurring schedule or Inactive if you do not want to set a schedule. If you choose Inactive, you cannot select a frequency or time.
Frequency	Select how often the report should run. This can be one of the following: • Daily • Hourly • Weekly
at	Enter the time when you want the report to run. This depends on your Frequency selection. • Daily—Select the time that you want the report to run. • Hourly—Select how many hours to wait before you run the report again. • Weekly—Select the days of the week and the time that you want the report to run.

8. Click **Create**.

Viewing Reports

The Manage Reports page displays all existing reports in your system. The reports are a high-level overview suitable for a management summary. All reports are generated as a PDF. You can generate the following types of reports:

- Executive Summary Report
- Licensing Report

To access the Manage Reports page, select **Reports** from the side menu bar.

The **Reports** tab displays all reports that have not been deleted. On this page, you can:

- Create a new report.
- Use the Filter bar to narrow down your results.
- Click the report name to view the report details and edit the report.
- Click the Last Run link to view the report.
- Click the icons at the end of each row to run the report without a schedule, edit the report, or delete the report.

The **History** tab displays all the report versions that do not exceed the retention period. On this page, you can:

- Use the Filter bar to narrow down your results.
- Click the icons at the end of each row to download the report or delete the report version.

8 Compliance

This section contains:

Deleting a Schedule

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Compliance page, select the **Schedules** tab.
4. On the Schedules tab, locate the schedule that you want to run and click the **Delete** icon.

Editing a Schedule

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Compliance page, select the **Schedules** tab.
4. On the Schedules tab, locate the schedule that you want to run and click the **Edit** icon.
5. Make any changes that you require and click **Save**.

Manually Running a Schedule

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Compliance page, select the **Schedules** tab.
4. On the Schedules tab, locate the schedule that you want to run and click the **Run Now** icon.

Creating a Schedule

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Compliance page, select the **Schedules** tab.
4. On the Schedules tab, click **Create Schedule**.
5. Enter the name and optional description for the schedule.
6. Chose whether the schedule should be Enabled or Disabled.
   Enabled policies will run automatically per the schedule or manually. You cannot run a disabled policy.

7. In the Policy section, select the category and the policy that you want to run.
8. In the Vaults section, add the vault or vaults that you want to run the policy against. The vault must be compatible with the selected policy.
9. In the Schedule, select the date and time that you want the schedule to run.
10. Click **Create**.

About Schedules

Schedules will automatically run a compliance policy against the defined vaults at the time that you set. You can manually run a schedule at any time.

Deleting a Custom Compliance Policy

You can only delete custom compliance policies. System policies are read-only. The Edit and Delete icon for each custom policy is only visible when you highlight the policy.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Policies page, highlight the policy that you want to delete and click the **Delete** icon.

The policy is immediately deleted.

Modifying an Existing Compliance Policy

If you are modifying a custom policy, you can save it directly. If modifying a system policy, you must save it under a different name and then open the policy.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
3. On the Policies page, select the policy that you want to modify.
   Note: For system policies, click **Save As**, enter a new policy name and optional description, and click **Save**. Select the new policy from the Policies page.
4. Review the operations that exist for the policy. You can edit or delete the operations.
5. Click **Add Operations**.
6. In the Add Operation window, select the catalog or policy from which you would like to add operations. All operations available in the catalog or policy will be displayed beneath the policy.
7. Select the operations that you would like to add and click **Add** or **Add & Close**.
8. If you clicked **Add**, repeat the previous step. Click **Add & Close** when you are finished.
9. Edit the parameters for each operation that you have added.
10. When you have finished, click **Save**.

Creating a Compliance Policy

If you only want to modify operation parameter values in an existing system policy, we recommend that you save a copy of that policy instead of creating a new one.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance.**
3. Click the **Create Policy** button.
4. In the Create Policy window, enter the name of the policy. This name can be modified later.

5. Enter an optional description to help identify the policy.
6. Select the object type that will be included in the policy
7. Click **Add Operations**.
   The Cryptographic Security Platform Compliance Manager takes you to the Policies page for your new policy.
8. On the Policies page, click **Add Operations**.
9. In the Add Operation window, select the catalog or policy from which you would like to add operations.
   All operations available in the catalog or policy will be displayed beneath the policy.
10. Select the operations that you would like to add and click **Add** or **Add & Close**.
11. If you clicked **Add**, repeat the previous step. Click **Add & Close** when you are finished.
12. Edit the parameters for each operation that you have added.
13. When you have finished, click **Create**.

Post-Quantum Compliance

Compliance Manager now supports Post-Quantum Cryptography (PQC) with NIST aligned guidelines. The Entrust Post Quantum Reference Policy allows you to check if an asset is in compliance with post-quantum (PQ) cryptographic standards by validating the algorithms used. This policy contains the following operations:

- Verify Not Quantum Safe Cryptographic Algorithm—This operation checks to see if the algorithm being assessed is found in the Not Allowed PQ Algorithm list.
  - If the algorithm **is** on the list, then it is not allowed, and the operation will fail.
  - If the algorithm **is not** on the list, then it is allowed, and the operation will pass.
- Verify Quantum Safe Cryptographic Algorithm—This operation checks to see if the algorithm being assessed is found in the Allowed PQ Algorithm list.
  - If the algorithm **is not** on the list, then it is not allowed, and the operation will fail.
  - If the algorithm **is** on the list, then it is allowed, and the operation will pass.

The Allowed and Not Allowed lists have sample values in them, but you can edit them to meet your requirements.

Viewing Compliance Policies

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Compliance**.
   The Policies page displays. The Policies page contains a list of all policies and can be sorted by the following:
   - The name of the policy
   - The optional description of the policy
   - The type of object for which the policy is meant
   - Whether the policy is a System or Custom policy.
     Note: System policies are read-only. Open a system policy and click **Save As** to keep any changes that you make.
   - The number of operations contained in the policy
   - The date the policy was last updated
3. Select the policy that you want to view.
   The individual policy page displays the operations contained in the policy and whether they are enabled and/or configured. From here you can:
   - Click **Edit** to make changes to an operation. If the policy is a system policy, you'll need to save it as a custom policy to keep any changes.
   - Click **Delete** to remove the operation from this policy.
4. Click **Cancel** to return to the Policies page.

About Compliance

On the Compliance page, you can manage the compliance policies and schedules that you want to apply to your vaults. Entrust creates sample policies which include operations and parameters for those operations. There are two types of policies:

- System—System policies are created by Entrust as a reference and cannot be modified. However, you can save them as a custom policy.
- Custom—Custom policies include Best Practice policies that are created by Entrust and policies that you have created yourself. You can either create a policy by saving a system policy under a different name, or create a policy from scratch.

All policies can be run by adding them to a schedule. Schedules automatically run a selected policy against a specified vault at the time you choose. You can also choose to run a schedule immediately.

9 Documentation

This section contains:

Deleting a Custom Template

System templates cannot be deleted. The Edit and Delete icon for each custom template is only visible when you highlight the template.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select Documentation.
3. On the Templates page, highlight the template that you want to delete and click the **Delete** icon.

The template is immediately deleted.

Modifying a Template

System templates cannot be modified, however you can save them as a new template under a different name.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select Documentation.
3. On the Templates page, select the template that you want to modify.
4. On the template page, click **Edit Template**.
   On the template page, you can now add or remove metadata, edit fields, or delete fields.
   Note: If a field is referenced by a compliance policy, you cannot edit the field.
   - Click **Reorder Fields** to change the order that the fields are listed in.
   - Click **Add Field** to add a new field to the template.
5. If the template is a System template, click **Save As** and enter the new name and optional description of the template, then click **Save**.
6. If the template is not a system template, you can click **Save** to update the template with the existing name, or **Save As** to change the name.
7. Click **Cancel** to exit without saving.

Assigning a Documentation Template

Documentation templates are assigned to an individual vault.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Vaults**.
3. Select the vault for which to assign a documentation template.
4. Click the Documentation tab.
5. Select the documentation template and click **Apply**.

Creating a Documentation Template

Documentation templates contain information that helps you identify and run compliance reports against your cryptographic assets.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select Documentation.
3. Click the **Create Template** button.
4. In the Create Template window, enter the name of the template. This name can be modified later.
5. Enter an optional description to help identify the template.
6. Select the category type that will be included in the template.
   The Cryptographic Security Platform Compliance Manager takes you to the Templates page for your new template.
   On the Templates page, you can add metadata and user input fields to help identify the cryptographic assets.
7. In the Metadata field, select the metadata that you would like to add to the template. Click **x** to remove any metatdata that you do not want to use.
8. Click **Add Field**.
9. Choose one of the following:
   - Browse Catalog—Choose an existing field from the catalog and modify it to meet your specifications.
   - Custom Field—Create the fields you want from the provided options.
10. Follow the on screen instructions to create or modify your fields.
11. Click **Add** to add the field and create an additional field, or **Add & Close** to add the field and close the window.
12. When you have finished adding all of your fields, click **Save**.

Viewing Documentation Templates

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select Documentation.
3. On the Templates page, you can view all of the document templates have been created.
   System templates are created by Cryptographic Security Platform Compliance Manager, and cannot be modified. Custom templates can be edited or deleted.

About Documentation

Documentation allows you to track information about the cryptographic assets contained in each data source. The owners of the cryptographic assets will need to manually complete the documentation for their objects.

Cryptographic Security Platform Vault uses templates to determine which information must be collected for the cryptographic assets. By default, we supply several documentation templates that you can use as is or modify under a different name. You can also create a template from scratch.

10 Appliance Clusters

This section contains:

About Appliance Clusters

Appliance clusters are the cluster nodes that contain the Cryptographic Security Platform Vault that you want to monitor in Cryptographic Security Platform Compliance Manager.

Note: If you are creating a new cluster, or your cluster is degraded and you replace the affected node, the Cryptographic Security Platform Appliance Management webGUI may show that the cluster is healthy, but it may still take up to 30 minutes to restore all functionality.

Creating an Appliance Cluster Connection

Appliance clusters consist of all of the individual cluster nodes for the Cryptographic Security Platform Vault appliance. If you want to add an individual vault, for example, the Cryptographic Security Platform Vault for KMIP, select **Data Sources** from the side menu bar. You need to create a connection with the Appliance Cluster to view the cluster in the Cryptographic Security Platform Compliance Manager.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Appliance Clusters**.
3. Select **Actions > Initialize Connection**.
4. On the Initialize Connection to a Cluster page, enter the appliance URL for one of the nodes of a Cryptographic Security Platform Vault.
   Note: The appliance URL can be found by logging into the Cryptographic Security Platform Vault Management appliance, and then clicking Switch to Appliance Management in the top right corner. The URL should be similar to https://<IP_Address>/appliance/.
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 appliance cluster.
   Important: This file should be considered a password. Please save it in a safe location in case you need to reconnect the same appliance cluster.
6. Log into the Cryptographic Security Platform Vault that you created the connection to.
7. At the top of the page, you will see a warning that you are not connected to Cryptographic Security Platform Compliance Manager. Click **Connect Now**.
8. Click **Connect** and upload the JSON file that you downloaded from Cryptographic Security Platform Compliance Manager.
9. Click **Close** to close the Connect CSP Compliance Manager window.

Viewing Appliance Cluster Details

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Appliance Clusters**.
3. Select the cluster that you want to view.
   The Appliance Cluster Details window displays the following:

- the connection status
- the date and time of the last sync
- the IP address of the Cryptographic Security Platform Vault cluster
- the installed software version
- the date the connection was established

4. Click **Close** to close the window.

11 Compliance Manager Authentication and Settings

The Settings page consists of the following tabs:

- About—Allows you to view the name and UID of this Compliance Manager tenant and add an image.
- Members—Allows you to invite a user and assign them a role.
- Local Users—Allows you to manage local users.
- Authentication—Allows you to configure Active Directory or OIDC authentication.

This section contains:

Configuring OpenID Connect

Cryptographic Security Platform Compliance Manager supports user authentication through an OpenID Connect provider. Once enabled, you will log in using the OIDC provider.

Before You Begin

The OpenID Connect provider must be configured to accept the Cryptographic Security Platform Compliance Manager URIs for each node of the cluster. The URIs are located in the Cryptographic Security Platform Compliance Manager webGUI for each tenant. The Client ID and Client Secret are located in the OIDC provider. For more information, see External Authentication Providers.

Procedure

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Authentication** tab.
4. In the OpenID Connect section, click **Configure**.
5. In the Disable Local Authentication dialog box, click **Continue**.
6. Enter the following:

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Compliance Managerdisplays 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.

Field	Description
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	Enter the base URL. For Entrust IDaaS, the base URL will be: https://<IDaaS server>/api/oidc
Admin Name	The name of the tenant administrator.
Admin Email	The email address of the tenant administrator.

7. Click **Apply**.

Reconfiguring Active Directory

After you have successfully configured Active Directory, you can reconfigure it. This will wipe out the current Active Directory settings and start a new configuration.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Authentication** tab.
4. On the Authentication tab, click **Manage** under Active Directory.
5. In the Authentication > Manage Active Directory section, click **Reconfigure AD Now**.
6. In the Details section, enter the following:

Field	Description
Configuration Method	Choose whether to use Automatic or Manual configuration.
Domain Name	The Domain name to use for account authentication.
Security	Choose None or SSL.
Service Account	The AD account that the tenant should use when logging into the AD server.
Service Account Password	The password for the Service Account.

7. Click **Next**.
8. If you selected Automatic configuration, do the following:
    a. In the Domains section, verify the domain that you want to use. The default domain is displayed with a star icon.

Important: Cryptographic Security Platform Compliance Manager automatically adds all of the discovered domain controllers and global catalogs, starting with the closest. If you have a large number, then this will be done in the background. If the domain that you want to use is not visible, and you do not want to wait, then we recommend that you complete the configuration process, then edit your AD configuration later.

b. Click **Next** and proceed to step 10.

9. If you selected Manual configuration, do the following:
   a. In the Domains section, click the **Edit** icon to add at least one domain controller and global catalog.
   b. Click **Add Domain Controller** in the Edit Domain bar.
   c. In the Add Domain Controller section, complete the following:

Field	Description
Name	Enter the name of the domain controller.
Port	Enter the port number for the domain controller.
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	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.

   d. Click **Add Global Catalog** in the Edit Domain bar.
   e. In the Add Global Catalog section, complete the following:

Field	Description
Name	Enter the name of the global catalog.
Port	Enter the port number for the global catalog.
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	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.

f. Click **Update**.
g. Click **Next**.

10. In the Administrator section, enter the following:

Field	Description
Domain	Enter the name of the domain.
User	Enter the name of the Active Directory user.

11. If you are using SSL for security, click **Next**. If not, proceed to step 13.
12. In the Certificates section, check the **Approve All Certificates** checkbox. This will automatically approve all of the certificates in the domain controllers. Approving a certificate will download and approve all related certificates.
13. Click **Complete**.

You are logged out of the Cryptographic Security Platform Compliance Manager webGUI and can log back in with your AD credentials.

Configuring Active Directory

If you want to specify AD-managed Security groups whose members will have access to Cryptographic Security Platform Compliance Manager, you must specify a Windows Active Directory (AD) server.

Cryptographic Security Platform Compliance Manager 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.

Note: Configuring Active Directory will disable Local Authentication.

Procedure

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Authentication** tab.
4. In the Active Directory section, click **Configure**.
5. In the Disable Local Authentication dialog box, click **Continue**.
6. In the Details section, enter the following:

Field	Description
Configuration Method	Choose whether to use Automatic or Manual configuration.
Domain Name	The Domain name to use for account authentication.
Security	Choose None or SSL.
Service Account	The AD account that the tenant should use when logging into the AD server.

Field	Description
Service Account Password	The password for the Service Account.

7. Click **Next**.
8. If you selected Automatic configuration, do the following:
    a. In the Domains section, verify the domain that you want to use. The default domain is displayed with a star icon.
    Important: Cryptographic Security Platform Compliance Manager automatically adds all of the discovered domain controllers and global catalogs, starting with the closest. If you have a large number, then this will be done in the background. If the domain that you want to use is not visible, and you do not want to wait, then we recommend that you complete the configuration process, then edit your AD configuration later.
    b. Click **Next** and proceed to step 10.
9. If you selected Manual configuration, do the following:
    a. In the Domains section, click the **Edit** icon to add at least one domain controller and global catalog.
    b. Click **Add Domain Controller** in the Edit Domain bar.
    c. In the Add Domain Controller section, complete the following:

Field	Description
Name	Enter the name of the domain controller.
Port	Enter the port number for the domain controller.
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	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.

    d. Click **Add Global Catalog** in the Edit Domain bar.
    e. In the Add Global Catalog section, complete the following:

Field	Description
Name	Enter the name of the global catalog.
Port	Enter the port number for the global catalog.

Field	Description
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	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.

f. Click **Update**.
g. Click **Next**.

10. In the Administrator section, enter the following:

Field	Description
Domain	Enter the name of the domain.
User	Enter the name of the Active Directory user.

11. If you are using SSL for security, click **Next**. If not, proceed to step 13.
12. In the Certificates section, check the **Approve All Certificates** checkbox. This will automatically approve all of the certificates in the domain controllers. Approving a certificate will download and approve all related certificates.
13. Click **Complete**.

You are logged out of the Cryptographic Security Platform Compliance Manager webGUI and can log back in with your AD credentials.

Adding and Deleting Local Users

Local authentication is configured by default with the tenant administrator as a member.

Adding Local Users

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click **Local Users** to view your existing users.
4. Click **Create User**.
5. Enter the email address and the name for the new local user.
6. Click **Create User**.

Deleting Local Users

Note: For local authentication, you cannot delete a local user until it has been removed from the Members tab.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click **Local Users** to view your existing users.
4. Highlight the user that you want to delete and click the **Delete** icon.
5. In the Delete User window, click **Yes, Delete**.

Single Sign-On (SSO) Authentication

Cryptographic Security Platform Compliance Manager has added Single Sign-On (SSO) authentication. The account credentials that you set up for your specific authentication mode (local mode, OIDC, AD) for the Default tenant can now be used to log in to the Compliance Manager and Tenant Management appliances.

Note: When you log into the Compliance Manager and Tenant Management appliances, there are two options:

- If you have the Administrator role, you can login with your default credentials.
- If you are the secroot user, you can log in as secroot.

Adding and Removing Active Directory (AD) Members

A member can be either an administrator that can manage all collections or an auditor that only has view access of all collections. It is recommended to have at least two administrators.

Adding a Member

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Members** tab to view your existing members and their roles.
4. Click **Add Member**.
5. On the Add Member page, enter the AD domain, the name of the user that you want to add, and their email address.
6. Select whether the new member will be an administrator or an auditor.
7. If you selected Administrator, choose the additional roles that you would like to assign to this tenant.
    - Compliance Manager appliance and Tenant Management Administrator—Grants administrative access to the Appliance and Tenant Management applications.
8. Click **Add Member**.
   If SMTP is enabled, the new user will receive an email with the login URL for Cryptographic Security Platform Compliance Manager webGUI. If SMTP is not enabled, you will need to send the login URL to the new user.

Removing a Member

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Members** tab.
4. Highlight the member that you want to remove, and click the **Delete** icon.
5. In the Remove Member window, click **Yes, Delete**.

Inviting and Removing Local Authentication or OpenID Connect (OIDC) Members

A member can be either an administrator that can manage all collections or an auditor that only has view access of all collections. It is recommended to have at least two administrators.

Note: If you are using local authentication, members must be existing local users. This means you must add a local user before you can invite them to be a member, and remove them as members before you can delete them from the Local Users page.

Inviting a Member

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Members** tab to view your existing members and their roles.
4. Click **Invite Member**.
5. On the Invite Member page, enter the name of the user that you want to add and their email address.
6. Select whether the new member will be an administrator or an auditor.
7. If you selected Administrator, choose the additional roles that you would like to assign to this tenant.
    - Compliance Manager appliance and Tenant Management Administrator—Grants administrative access to the Appliance and Tenant Management applications.
8. Click **Invite Member**.
   For Local Authentication: If SMTP is enabled, the new user will receive an email with the login URL and a temporary password for the Cryptographic Security Platform Compliance Manager webGUI. If SMTP is not enabled, you will need to send the login URL and temporary password to the new user.
   For OIDC: If SMTP is enabled, the new user will receive an email with the registration URL. This URL is active for 24 hours only, and the user must click on the URL and sign in with their credentials before logging in to the Cryptographic Security Platform Compliance Manager webGUI. If SMTP is not enabled, you will need to send the registration URL to the new user.

Removing a Member

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **Members** tab.
4. Highlight the member that you want to remove, and click the **Delete** icon.
5. In the Remove Member window, click **Yes, Delete**.

Adding an Image

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the side menu bar, select **Settings**.
3. Click the **About** tab.
4. Click **Select Image**.
5. Select the image that you want to use to represent this app.
6. Click **Apply**.

12 Licensing and Entitlements

This section contains:

About Licenses and Entitlements

When you first start using your Cryptographic Security Platform Compliance Manager tenant, a trial license is installed by default. The trial license is valid for 30 days, and includes all data sources that you add to your collections. All entitlements are tracked in the Cryptographic Security Platform Compliance Manager. For the Cryptographic Security Platform Vault, all vault-related enforcement occurs in the Cryptographic Security Platform Vault.

Important: Entitlements are only available through the Cryptographic Security Platform Compliance Manager webGUI.

Adding a License

To add a license, you must log in to a Cryptographic Security Platform Compliance Manager tenant.

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the top-right corner, click the question mark (**?**) and select **License**.
3. Click the **Licenses** tab.
4. Click **Add License**.
5. Add your license in one of the following ways:
    - Import File
        i. Click the Import File radio button.
        ii. Click **Browse** and select the license file.
        iii. Click **Add**.
    - Enter License
        i. Click the **Enter License** radio button.
        ii. Paste the license into the text box.
        iii. Click **Add**.

Viewing Entitlements and Licenses

To view your entitlements and licenses, you must log in to a Cryptographic Security Platform Compliance Manager webGUI.

License counts are updated once daily, as well as:

- When a data source has been added to Cryptographic Security Platform Compliance Manager.
- When a Cryptographic Security Platform Vault cluster is deleted.
- When cryptographic assets are synced.
- When cryptographic assets are marked dormant.

Note: Cryptographic assets count differently depending on their state. For example, if a key has been rotated and has multiple versions, it will show up as one key in inventory, but the entitlement count is based on the number of keys that are pre-active, active, or available. Keys that have been archived or disabled only count as

1/10th of a key. Key fractions are rounded down, so if you have 19 disabled cryptographic assets, it will count as 1 asset. 20 disabled cryptographic assets will count as 2 assets.

Procedure

1. Log into the Cryptographic Security Platform Compliance Manager webGUI with your standard account credentials.
2. In the top-right corner, click the question mark (**?**) and select **Entitlements**.
   The Entitlements page displays the names of your entitlements, the limit, and how many are currently in use
3. In the Entitlements tab, you can view the names of your entitlements, the limit, and how many are currently in use.
4. In the Licenses tab, you can view the license activation keys, expiration date, and status.
5. Click the Activation key to view additional details about the license.

13 External Authentication Providers

This section contains:

Example: Configuring Azure OIDC to use with CSP Compliance Manager

The following example shows how to configure Azure OIDC to use with Cryptographic Security Platform Compliance Manager for External Authentication using Open ID Connect. You will need to register Entrust Cryptographic Security Platform Compliance Manager as a Microsoft Azure application, then copy the Client Secret, the Application (client) ID, and the base URL from Azure and paste it into Cryptographic Security Platform Compliance Manager.

1. In Microsoft Azure, click **App Registrations** in the sidebar.
2. Click **New Registration**.
3. In the Register an application page, enter the name to use for the application and enter the following redirect URIs.
    - Set the Login Redirect URIs for all nodes in the cluster to:
      `https://<IP or FQDN of Cryptographic Security Platform Compliance Manager node>/hytrust-authentication-rest/api/v2/login/`
    - Set the Logout Redirect URIs for all nodes in the cluster to:
      `https://<IP or FQDN of Cryptographic Security Platform Compliance Manager node>/hytrust-authentication-rest/api/v2/sso/logout/`
4. Click **Register**.
   After the application is created, you will be taken to the new application page.
5. Copy the Application (client) ID to a text window for later use.
   This will be the application (client) ID used in Cryptographic Security Platform Compliance Manager.
6. Click **Certificates & secrets** in the sidebar to create a client secret.
7. In the Client secrets section, click **New client secret**.
8. In the Add a client secret window, enter a description, set the expiration date, and click **Add**.
   The new client secret appears in the Client secrets section.
9. Copy the client secret value to a text window for later use.
   This will be the client secret used in Cryptographic Security Platform Compliance Manager.
10. Click **Token configuration** in the sidebar and then click **Add optional claim**.
11. In the Add optional claim window, select 'ID' for the token type and 'upn' and 'sid' for the claim.
12. Click **Add**.
13. In the pop-up window, check the 'Turn on the Microsoft Graph profile permission (required for claims to appear in token) checkbox.
14. Click **Overview** in the sidebar, and then click **Endpoints**.
15. In the Endpoints window, copy the OpenID Connect metadata document (up to and including the v2.0) to a text window to find the OpenID Connect URI or Issuer URI.
    For example, https://login.microsoftonline.com/a995284f-7628-4646-b755-ja0e3c7f0264/v2.0/. The '/.well-known/openid-configuration/' section is not needed.
    Note: This will be the base URL used in Cryptographic Security Platform Compliance Manager.
16. Close the Endpoints window to return to the Overview page.

Example: Configuring Entrust Identity as a Service

The following example is configuring Entrust Identity as a Service (IDaaS) to use with Cryptographic Security Platform Compliance Manager for External Authentication using OpenID Connect.

1. Log into Entrust IDaaS with your user name and one time password (OTP).
2. After you have logged in, click **Applications**.
3. Click the + icon to create a new Generic OpenID Connect and OAuth Cloud Integration.
4. Create a Generic Web Application using the following:
    - General Settings:
        - Copy and paste the Client ID and the Client Secret to a safe location. These will be used when configuring OIDC in Cryptographic Security Platform Compliance Manager.
        - Set the Token / Revocation Endpoint Client Authentication Method to Client Secret Post.
        - Set the Login Redirect URIs for all nodes in the cluster to:
          `https://<IP or FQDN of Cryptographic Security Platform Compliance Manager node>/hytrust-authentication-rest/api/v2/login`
          The URIs are located in the Cryptographic Security Platform Compliance Manager webGUI for each tenant.
        - Set the Logout Redirect URIs for all nodes in the cluster to:
          `https://<IP or FQDN of Cryptographic Security Platform Compliance Manager node>/hytrust-authentication-rest/api/v2/sso/logout`
          The URIs are located in the Cryptographic Security Platform Compliance Manager webGUI for each tenant.

      Important: If you use an IP address in the login and logout URLs, you can only log in to your Cryptographic Security Platform Compliance Manager tenant using the IP address. If you use the FQDN in the login and logout URLs, you can only log in to your Cryptographic Security Platform Compliance Manager tenant using the FQDN.
    - Authentication Settings:
        - Check the Require Consent checkbox.
        - Under Grant Types Supported, check the Authorization Code checkbox.
    - Supported Scopes
        - Select the Your unique identifier checkbox.
        - Select the Email address checkbox.

    Use the default for all other settings.
5. Add a resource rule to the AD Group so that the AD group and users from that AD group can access the application.

14 System Console

This section contains:

Exiting the Console

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Quit TUI session`.

Manage Timeouts and Appearance

In the Cryptographic Security Platform Compliance Manager System Console, you can set your TUI, GUI, and SSH session timeouts, as well as the TUI 3D appearance.

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Manage Timeouts and Appearance`.
3. On the Manage TUI Timeout and Appearance page, select one of the following and then select **OK**:
    - `Manage TUI Session Timeout`
      Allows you to change the TUI session timeout. The TUI timeout can be between 60 and 86400 seconds.
        i. Enter the new timeout value and select **OK**.
        ii. Review the new timeout value and select **OK** to return to the **Manage Timeouts and Appearance** page.
    - `Toggle TUI 3D Appearance`
      Selecting this option automatically updates the appears of the TUI.
    - `Manage GUI Settings`
      Allows you to change the Web Session (also called the GUI session) Idle Timeout. The default is 15 minutes. The maximum allowed is 1440 minutes.
        i. Enter the new timeout value and select **OK**.
        ii. Review the new timeout value and select **OK**.
        iii. Select Return to Previous Menu to return to the **Manage Timeouts and Appearance** page.
    - `Manage SSH Session Idle Timeout`
      Allows you to change the SSH Session idle timeout value. The default is 15 minutes.
        i. Enter the new timeout value and select **OK**. Enter 0 to disable timeouts.
        ii. Review the new timeout value and select **OK** to return to the **Manage Timeouts and Appearance** page.

Recover Compliance Manager Cluster

If your Cryptographic Security Platform Compliance Manager system is not responding, you can reset the cluster.

Important: This operation can take a long time.

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Manage Cryptographic Security Platform Compliance Manager Node`.
3. Select `Recover Compliance Manager cluster`.
4. Select `Yes` to proceed.

Delete CSP Compliance Manager Snapshots

Cryptographic Security Platform Compliance Manager automatically creates a pre-upgrade snapshot whenever you upgrade to a newer version. You can delete these pre-upgrade snapshots.

Important: If you delete the pre-upgrade snapshots, you cannot revert your upgrade to the previous installed version.

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Manage Cryptographic Security Platform Compliance Manager Node`.
3. Select `Delete Cryptographic Security Platform Compliance Manager pre-upgrade snapshot`.
4. In the confirmation screen, select **Yes**.

Change the secroot Account

The default user for the Cryptographic Security Platform Appliance Management webGUI is secroot. If the secroot user can no longer remember their credentials or is locked out, you can reset their credentials with a temporary password.

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Support Accounts`.
3. Select `secroot(Cryptographic Security Platform Compliance Manager webGUI default account)`.
4. Select one of the following:
   - If email is enabled, select **Generate random password and send it via email to secroot (Recommended)**.
     After receiving the email, the secroot user can log into the Cryptographic Security Platform Appliance Management webGUI and reset their password.
   - If email is not enabled, select **Enter new temporary password for secroot**.
     You will need to communicate the new password to the secroot user. After that, the secroot user can log into the Cryptographic Security Platform Appliance Management webGUI and reset their password.
5. Select `Return to previous menu` when you are finished.

Manage Read Only Support Access

The htrestricted account provides read-only access to debug Cryptographic Security Platform Compliance Manager.

Enabling the Support User

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Accounts`.
3. Select `htrestricted (read only support access)`.
4. Select Yes to enable the htrestricted account.

5. Enter and confirm a password for the Entrust support user.
   The password must be at least 8 characters long and must include at least one lowercase letter, one uppercase letter, one digit, and one symbol.
   Note: The password is only valid for 24 hours. The account is automatically disabled after 24 hours, or you can disable it when no longer needed.
6. Exit the console, and then log back in as htrestricted with the password that you created. You can also use an ssh client.

Entrust Support can now assist you further.

Disabling the Support User

The htrestricted user password will automatically expire in 24 hours. You can disable the support user at any time before that.

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Accounts`.
3. Select `htrestricted(read only support access)`.
4. Select Yes to disable the htrestricted account.

Manage Full Support Access

The htsupport user allows Entrust support to access your system. You can enable and disable the support user.

Enabling the Support User

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Support Accounts`.
3. Select `htsupport (full support access)`.
4. Select Yes to enable the htsupport account.
5. Enter and confirm a password for the Entrust support user.
   The password must be at least 8 characters long and must include at least one lowercase letter, one uppercase letter, one digit, and one symbol.
   Note: The password is only valid for 24 hours. The account is automatically disabled after 24 hours, or you can disable it when no longer needed.
6. Exit the console, and then log back in as htsupport with the password that you created. You can also use an ssh client.

Entrust Support can now assist you further.

Disabling the Support User

The htsupport user password will automatically expire in 24 hours. You can disable the support user at any time before that.

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Support Accounts`.
3. Select `htsupport (full support access)`.
4. Select Yes to disable the htsupport account.

Manage htadmin Account and SSH Access

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Manage htadmin and SSH Access`.
3. Select one of the following:

Option	Prompt	Description
1	Change htadmin Account Password	Select to change your htadmin password. a. Enter the current password at the prompt. b. Enter your new password. The password must be at least 8 characters long and must include at least one lowercase lett

Option	Prompt	Description
		er, one uppercase letter, one digit and one of the following special characters: ~, !, @, #, $, %, ^, &, *, (,), -, +. c. Reenter your new password. If the password was changed successfully, the console will display: Password successfully updated. If not, you will receive a message stating why the change was denied.

Option	Prompt	Description
2	Manage SSH Access to System Menu	Select to allow SSH login access to the htadmin account. You can enable or disable access.
3	Manage SSH Session Idle Timeout	Select to modify the SSH session idle timeout value. The default is 15 minutes. Select 0 to disable timeouts.

4. When you are finished, select `Return to Previous Menu`.

Manage your Network Settings

You can modify your network settings for standalone nodes and the primary nodes of a cluster.

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. Select `Manage Network Settings` and press Enter.
3. Select one of the following options:

Option	Prompt	Description
1	Show Current Network Configuration	Select to view your Cryptographic Security Platform Compliance Manager current network configuration.
2	Manage IP Address Settings	Select to change your current management interface. On the Interfaces page, select the network interface to configure and select OK. On the modify IP address settings, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. Click OK to return to the Manage Network Settings page.

Option	Prompt	Description
3	Disable a Network Interface	Select to disable a network interface.
4	Manage DNS Settings	Select to change your DNS settings. On the Modify DNS settings page, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. You are automatically returned to the Manage Network Settings page.
5	Manage NTP Settings	Select to change your NTP settings. On the Modify NTP network settings page, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. You are automatically returned to the Manage Network Settings page.
6	Manage Static Routes	Select to manage your static routes. See Manage your Static Routes.
7	Network Diagnostic Tools	Select to test your network connectivity. See Test Your Network Connectivity.

4. When you are finished, select `Return to Previous Menu`.

Manage Your Static Routes

You can view, add, or delete static routes.

Listing your Current Static Routes

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Network Settings` and press Enter.
3. On the Manage Network Settings page, select `Manage Static Routes` and press Enter.
4. On the Manage Static Routes page, select `List Current Static Routes` and select OK.

5. The current static routes are displayed. Select OK to return.

Adding a Static Route

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Network Settings` and press Enter.
3. On the Manage Network Settings page, select `Manage Static Routes` and press Enter.
4. On the Manage Static Routes page, select `Add Static Route` and select OK.
5. On the Add a static route page, enter the network address and gateway of the static route to add.
6. Select OK to save and return.

Deleting a Static Route

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Network Settings` and press Enter.
3. On the Manage Network Settings page, select `Manage Static Routes` and press Enter.
4. On the Manage Static Routes page, select `Delete Static Route` and select OK.
5. On the Delete a static route page, enter the network address and gateway of the static route to delete.
6. Select OK to save and return.

Test Your Network Connectivity

Cryptographic Security Platform Compliance Manager attempts to connect to different devices in your network and displays the connection information.

1. Log in to the Cryptographic Security Platform Compliance Manager as htadmin.
2. Select `Manage Network Settings` and press Enter.
3. On the Manage Network Settings page, select `Network Diagnostic Tools` and press Enter.
4. On the Network Diagnostics page, select one of the following and follow the prompts:
    - `Verify DNS Server Response`
    - `Verify NTP Server Response`
    - `Test Remote Server is Reachable`
    - `Test Inbound Ports of Another Server`
5. Select `Return to previous menu` when you are finished.

Setting 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 Compliance Manager webGUI, Cryptographic Security Platform Compliance Manager provides a self-service option using the Cryptographic Security Platform Compliance Manager 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 Compliance Manager webGUI with 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 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**.

Using the CSP Compliance Manager System Console

1. Log in to the Cryptographic Security Platform Compliance Manager System Console as htadmin.
2. In the Cryptographic Security Platform Compliance Manager System Console, enter your selection at the prompt. This can be one of the following:

Option	Prompt	Description
1	Manage Network Settings	Allows you to update your network settings. See Manage your Network Settings. **Note:** You cannot change networking settings for a cluster member.
2	Manage htadmin and SSH Access	Allows you to modify your htadmin pasword and SSH access. See Manage htadmin Account and SSH Access.
3	Manage Accounts	Allows you to enable Support access or change the secroot password. See Manage Full Support Access, Manage Read Only Support Access, or Change the secroot Account .
4	Manage HSM Client Account	If you are connecting Cryptographic Security Platform Compliance Manager to multiple HSM servers, this option allows you to configure those servers as an HA group..
5	Download Entrust Internal Certificate	Allows you to copy your CA certificate to a remote system. You will need to enter the remote system's hostname, username, and password.
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 Compliance Manager cluster.
7	Manage Cryptographic Security Platform Compliance Manager Node	Allows you to delete a Compliance Manager pre-upgrade snapshot or recover the kubernetes cluster. See Delete Compliance Manager Snapshots or Recover Cryptographic Security Platform Compliance Manager Cluster.

Option	Prompt	Description
8	Reboot or Shut Down Cryptographic Security Platform Compliance Manager Node	Allows you to reboot or shut down your Cryptographic Security Platform Compliance Manager instance. Choose whether to shut down or reboot Cryptographic Security Platform Compliance Manager, and then select Yes.
9	Manage Timeouts and Appearance	Allows you to set your TUI, GUI, and SSH session idle timeouts. See Manage Timeouts and Appearance.
10	Quit TUI Session	Exits the console. See Exiting the Console.

Accessing the System Console

The Cryptographic Security Platform Compliance Manager System Console is a TUI (Text-based User Interface), and is accessed by logging in as htadmin.

You can access the Cryptographic Security Platform Compliance Manager System Console using one of the following:

- the vCenter Server Console where you installed Cryptographic Security Platform Compliance Manager
- an SSH session using the htadmin account

Note: SSH is disabled by default. To modify the settings, see Manage htadmin Account and SSH Access.

15 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.

16 Copyright

Copyright and Legal Notice

Entrust Cryptographic Security Platform Compliance Manager® version 10.5.4

©2026 Entrust Corporation. All Rights Reserved.

Entrust Cryptographic Security Platform, Entrust Cryptographic Security Platform Vault, Entrust Cryptographic Security Platform Compliance Manager, Entrust Virtualization Under Control, Entrust CloudAdvisor, Entrust CloudControl, Entrust DataControl, Entrust KeyControl, and other Entrust product names are trademarks of Entrust. Other trademarks are recognized as belonging to their respective owners. The content of this guide is furnished for informational use only and is subject to change without notice. Entrust assumes no responsibility or liability for any errors or inaccuracies that may appear in the content contained in this guide. Except as allowed by license, no part of this material may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the written permission of the copyright owner, except where permitted by law.

U.S. Patent information: https://www.entrust.com/legal-compliance/patents.

Entrust 1187 Park Place Minneapolis, MN 55379 U.S.A. Phone 1 800-621-6972	Email: hytrust.support@entrust.com Website: https://www.entrust.com/digital-security/cloud-security-encryption-key-management