THALES

Thales Crypto Command Center 3.7.1

USER GUIDE

Document Information

Product Version	3.7.1
Document Part Number	007-012224-016
Release Date	09 December 2020

Revision History

Revision	Date	Reason
Rev. A	09 December 2020	Update

CONTENTS

007-012224-016 Rev. A 09 December 2020

About this Guide

This document describes how to install, configure, and use Thales Crypto Command Center 3.7.1. It contains the following sections:

- Overview
- Setting up a CCC Server
- Administration
- Service Deployment
- Troubleshooting

This section also includes the following information:

- Audience
- Document Conventions
- Contacting Thales Customer Support

Audience

This guide is intended for:

- Security Administrators who are responsible for managing the devices added to CCC and provisioning services on the added devices.
- Application Owners who are responsible for deploying and using the services with their cryptographic applications.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only. It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

Notes

Notes are used to alert you to important or helpful information. They use the following format:

> **NOTE** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Command Syntax and Typeface Conventions

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)

Format	Convention
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Contacting Thales Customer Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The customer support portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@thalesgroup.com.

CHAPTER 1:
Overview

This guide contains instructions for installing, configuring, administering, and managing Thales Crypto Command Center 3.7.1. Crypto Command Center (CCC) is a web-based application that enables you to provision, manage, and administer your Thales Luna Network HSMs on premises without compromising on the safety and compliance requirements. You can use CCC to:

- Deploy crypto resources quickly and efficiently to meet current and future encryption requirements.
- Generate dynamic reports, receive email alerts on service-impacting events, and remain up to date on the status of your HSM device pool.
- Discover and import unmanaged crypto resources, and dynamically reassign services.
- Create and deploy your own custom, repeatable crypto templates to enforce security and consistency.
- Deploy crypto resources in high availability to minimize downtime.

High-level Architecture

This section describes the architecture of CCC. It contains the following topics:

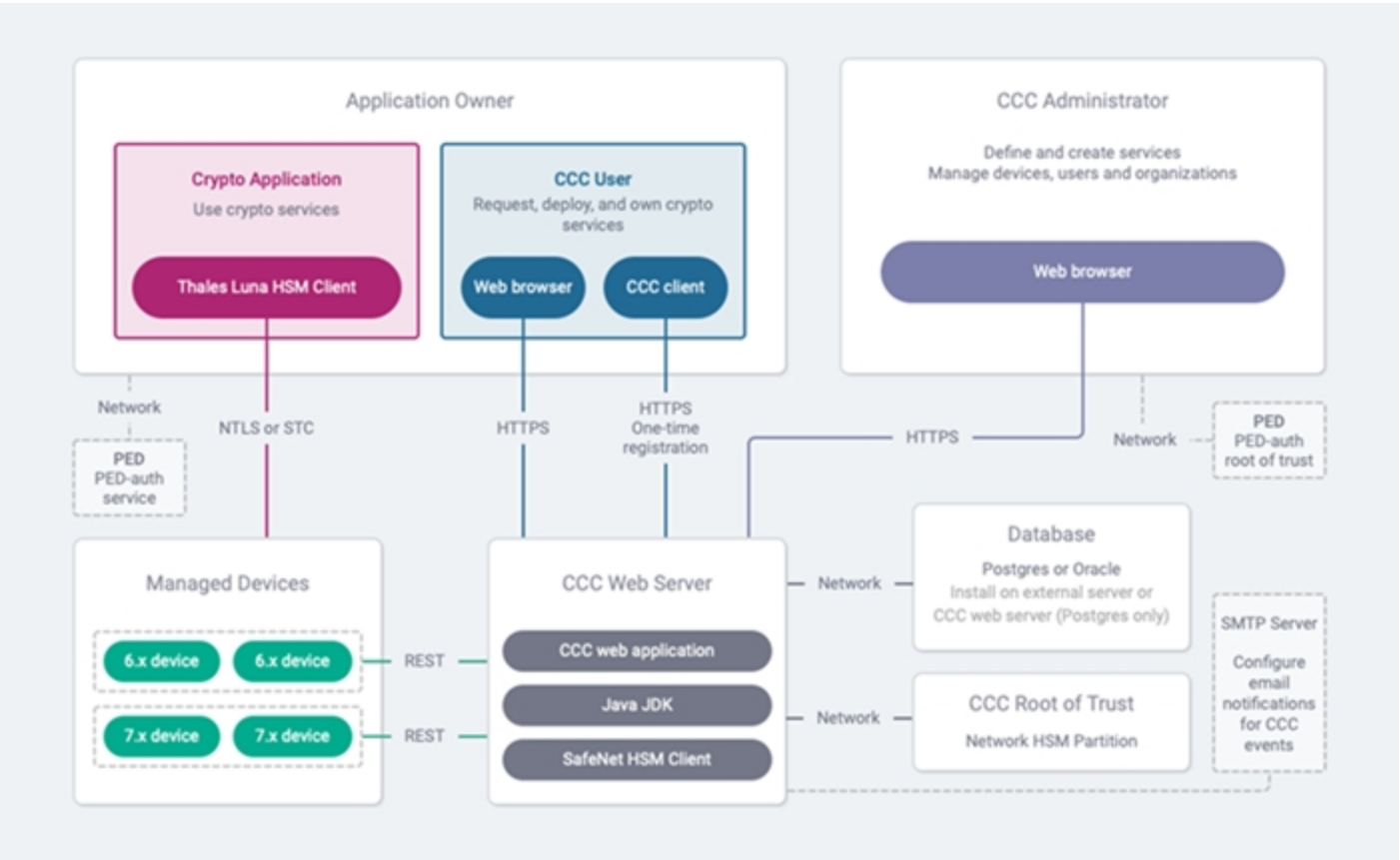
Overview

The following figure provides a high-level architectural view of CCC. Central to CCC is the CCC server. The CCC server is a Linux workstation where the CCC web application is installed. The CCC web application includes an application container and service, which provides the administrative and application owner interfaces for managing and deploying HSM resources.

In addition to the web application, CCC also requires the following components:

- A Thales Luna Network HSM to serve as the root of trust, to authenticate communications between the CCC and managed HSM devices.
- A PostgreSQL or Oracle database. The database can be installed either on the same server or on a different server used for hosting the CCC web application.

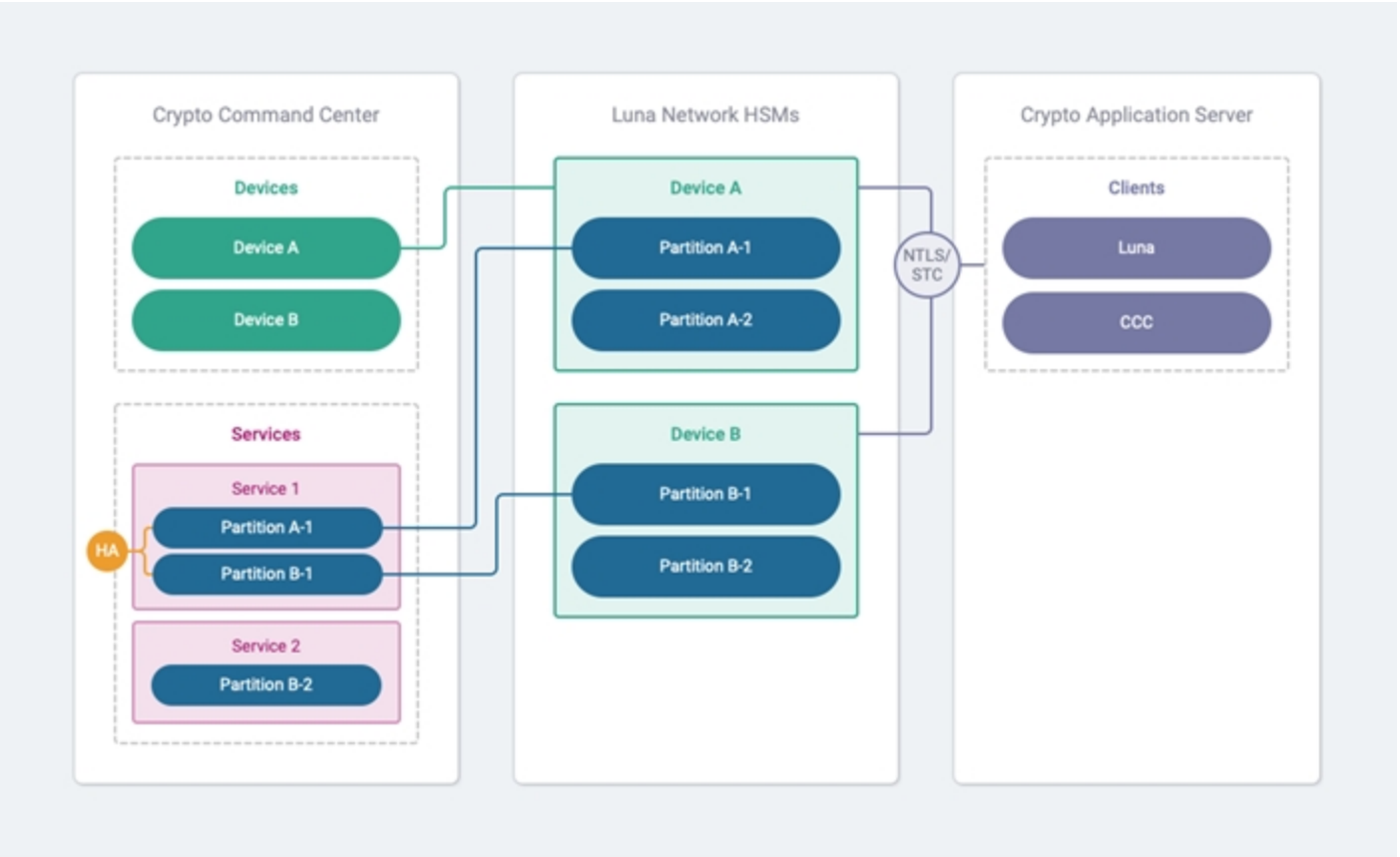
Figure 1: CCC High Level Architecture



Server and Client Components

CCC is installed on a Linux workstation running CentOS or Red Hat Enterprise Linux. The *Customer Release Notes* list specify supported versions of these operating systems. CCC also includes a Java client, which is used to deploy a service created in CCC on a crypto application server.

Figure 2: CCC High Level Diagram



Terms	References
Devices	Devices are referred as Luna Network HSMs.
Services	Services are referred as one or more partitions in Luna Network HSMs.
Clients	Clients are referred as Application owners who are responsible for deploying the services.

Web Server

The CCC web server consists of a Java-based web application. It uses the Java JDK and requires the Thales Luna Network HSM client software to communicate with the root-of-trust HSM.

Databases

The data managed by CCC is stored in a PostgreSQL or Oracle database. You can install the database on the CCC server, or on an external server.

Root-of-Trust HSM

All communications between CCC and the HSMs on any managed devices are authenticated using a Thales Luna Network HSM. You can use a password-authenticated or PED-authenticated Thales Luna Network HSM partition as the root of trust. You can use a FIPS-enabled HSM if FIPS compliance is required, or a non-FIPS-enabled HSM if you do not require FIPS compliance.

If the root-of-trust HSM is PED-authenticated, it must be activated (to allow password login) to work with CCC. You can activate (enable) or deactivate (disable) the root-of-trust HSM as required to control whether or not CCC has access to the HSMs on the managed devices to create and deploy services.

> **NOTE** Activation of a PED-authenticated HSM to allow password authentication is not the same as activation of CCC. Activation of CCC enables the root-of-trust HSM, which allows CCC to create and deploy services.

Crypto Command Center Client

The Crypto Command Center client is run on a crypto application server to set up the NTLS or STC links from the application server's Thales Luna Network HSM client to the devices used to host the service. STC links are available for devices with a minimum software version of 6.2.1 and a minimum firmware version of 6.24.2. The Crypto Command Center client is available for download from CCC.

Users

CCC supports two distinct user roles: Administrators, and Application Owners.

Administrators

Administrators are responsible for creating organizations, adding user accounts, adding devices, and creating services on the managed devices. Administrators can also generate reports for the managed devices and services.

Application Owners

Application owners are responsible for deploying the services created in CCC for their organization. Application Owners own the services and are free to deploy them as they see fit. When the services are no longer required, the Application Owner can release the service, making the resources used to provide the service available to the Administrator to create new services.

The following table compares the capabilities of the CCC Admin and CCC Application Owner users:

Feature	CCC Admin	CCC Application Owner
Service Creation	Yes	No
Service Initialization	Yes	Yes
Service Deployment	Yes	Yes
Key Material Visibility	Yes	Yes
Reporting	Yes	No
Service Monitoring	Yes	Yes
Device Monitoring	Yes	No
Alerting and Notifications	Yes	No
Licensing	Yes	No
Support Catalog	Yes	No

Software Center	Yes	Yes
Directory Support	Yes	No
Device Log Export	Yes	No
Account Management	Yes	No

Managed Devices

You can use CCC to manage Thales Luna Network HSM devices. CCC is able to manage any Thales Luna Network HSM device that is available over the network, including those located in the cloud. In order to manage a device, CCC must be able to log in to the device as the admin user. The admin credentials required to log in to the device are encrypted using an encryption key stored on the root-of-trust HSM, and stored in CCC.

Device Requirements

CCC can manage PED-authenticated and password-authenticated Thales Luna Network HSM devices. For CCC to manage a Thales Luna Network HSM device, the device must meet the minimum requirements, as specified under the Hardware and Software Requirements section.

Workflow

This section describes the workflow in CCC. It contains the following sections:

High-Level Workflow

The high-level workflow in CCC is outlined below and illustrated in the following figure.

Figure 3: CCC Workflow

1. Activate CCC to enable authenticated communications with the device HSMs. Activation is required to enable user management, device authorization, service creation, and reporting. See "Server Administration" on page 67.
2. Create user organizations and add users to the organizations. All application Owner users must belong to an organization. See "Account Management" on page 75.
3. Add devices and optionally group them into device pools. See "Device Management" on page 77.
4. Authorize CCC to log in to the devices as the HSM security officer (SO).

5. Import any partitions or partition HA groups that are already configured on the appliance, but that do not exist as services in CCC. You can perform this function at any time. See "Discovering and Importing Unmanaged Partitions" on page 87.
6. Create service templates to define the characteristics of the new services you want to create. All new services must be based on a template. See "Service Management" on page 84.
7. Create new services and assign them to an organization.
8. Initialize the new services. A new service can be initialized by the CCC Administrator or Application Owner.
9. Download the CCC client to the Thales Luna Network HSM client workstation you want to deploy the service on. The CCC client is available for download from CCC by Administrator or Application Owner users. See "Service Deployment" on page 140.
10. As an Application Owner that belongs to the organization that owns a new service, deploy the new service by running the CCC client on the Thales Luna Network HSM client workstation you want to deploy the new service on.
11. Begin using the new service with your cryptographic applications.

User Account Management

CCC Administrators can perform user account management tasks in activated mode only. The main steps are as follows:

1. Log in to CCC as the default Admin user.
2. Change the default password, if this is the first login.
3. Create additional Administrator users, if desired. Administrator users do not belong to an organization.
4. Create the organizations that will own the services you create.
5. Add user accounts for Application Owner users and assign them to an organization.

> **NOTE** Application Owner users can only be moved to a new organization by deleting them from their current organization and then adding them to a new organization.

See Account Management for detailed procedures that describe how to perform user account management tasks.

Device Management

CCC Administrators can perform device management tasks in activated mode only. The main steps are as follows:

1. Add the devices you want to manage. To add a device, you must specify the device address and admin login credentials.

   When you add a device, its capabilities are retrieved from the device, and stored in the database. If the device capabilities change, you can query the device to update the capabilities stored in CCC.
2. To help organize the devices, you optionally create device pools that can contain multiple devices.
3. Place the devices into device pools, if desired.
4. Authorize the devices.

See "Device Management" on page 77 for detailed procedures that describe how to perform device management tasks.

Administrators can generate, view, print, or export reports that provide detailed information for all of your managed devices. See "Reports" on page 111.

Service Management

CCC Administrators can perform service management tasks in activated mode only. The main steps are as follows:

1. Import any partitions or partition HA groups that are already configured on the appliance, but that do not exist as services in CCC. You can perform this function at any time.
2. Create service templates for each type of new service you wish to create.
3. Create new services and assign them to an organization.
4. Initialize the new service (Administrator or Application Owner user).

See "Service Management" on page 84 for detailed procedures that describe how to perform service management tasks.

Administrators can generate, view, print, or export reports that provide detailed information for all of your provisioned services. See "Reports" on page 111.

Service Deployment

Application Owners can deploy services created for their organization in activated mode only. The main steps are as follows:

1. Log on to CCC and initialize the service you want to deploy. Services can be initialized by the Administrator or Application Owner.
2. Download the CCC client to the Thales Luna Network HSM client workstation that will host the service.
3. Run the CCC client to select and deploy the service.
4. Begin using the service with your cryptographic applications.
5. Release the service when it is no longer required. The resources used to provide the service become available to CCC for creating new services.

See "Service Deployment" on page 140 for detailed procedures that describe how to deploy a service.

Authentication Model

This section describes how CCC authenticates users, devices, and HSM login sessions. It contains the following sections:

Overview

The user, device, and service management functionality provided by CCC requires it to store the following information:

> the user passwords for the CCC users. This information is used to control access to CCC. These passwords are hashed and stored in the database, and are not extracted from that location.

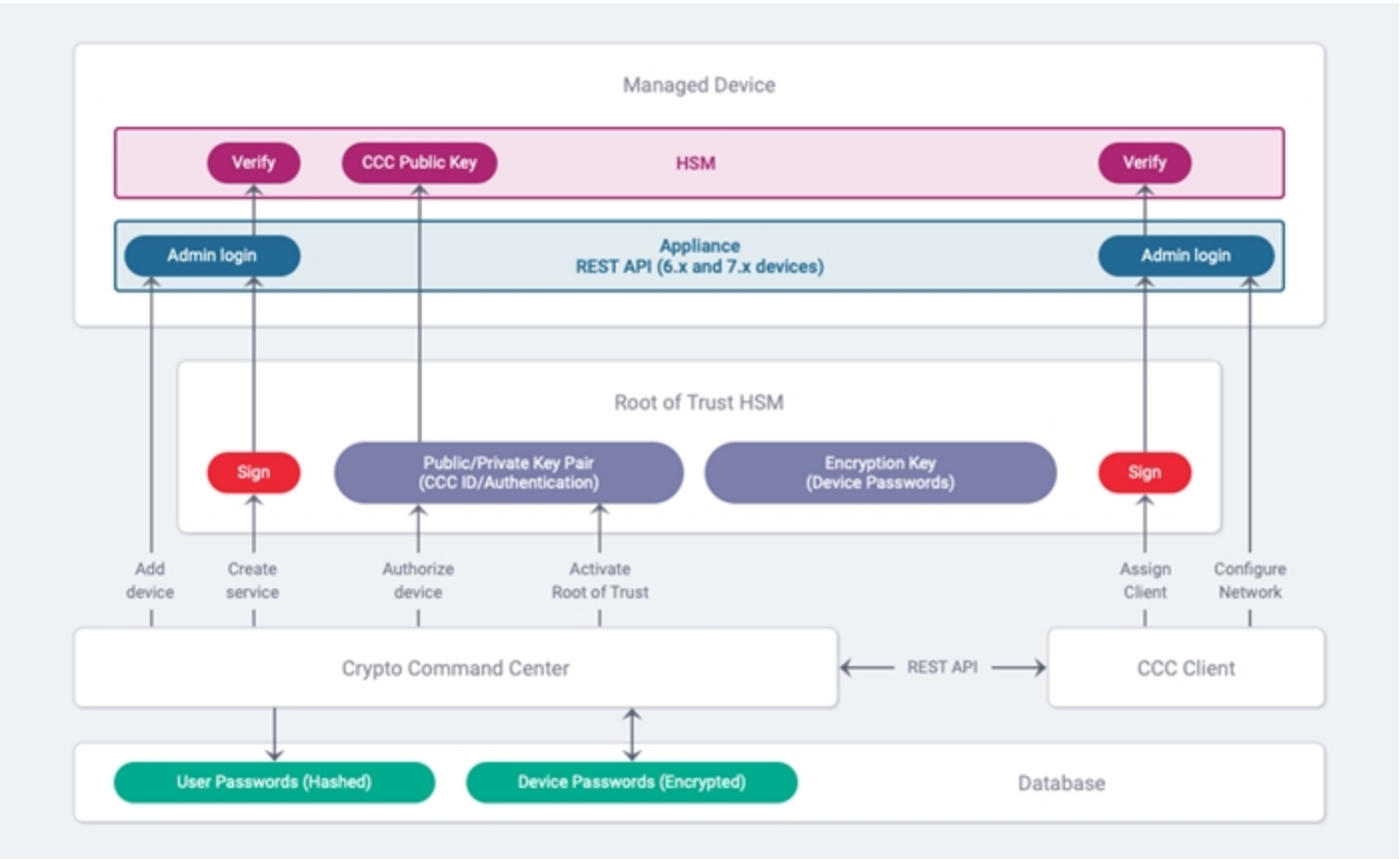
> **NOTE** CCC stores passwords for local users only. CCC does not store passwords for the users imported from a Directory.

> the Admin password for the managed devices. This information is used to allow CCC to log in to a managed device using REST API. The Admin password is encrypted using an encryption key stored in the root-of-trust HSM, before being stored in the database. When it is required to log in to a device, the password is extracted from the database and decrypted using the encryption key stored in the root-of-trust HSM.

In addition, all communications between CCC and the device HSMs are authenticated using a key pair stored on the root-of-trust HSM. The key pair is created when you first activate CCC. The public key is copied to the device HSM when you authorize a device. The private key is used to sign messages sent to the HSM. The public key is used to verify the messages received by the HSM.

The authentication model is illustrated below and described in detail in the following sections:

Figure 4: CCC Authentication Model



Password Management

CCC manages the following three types of passwords:

User passwords	User passwords (along with the user name) provide access to CCC, either as an Administrator or as an Application Owner. These passwords are used only by CCC, and do not need to be extracted from the database to be passed to another application. Because they are not extracted, these passwords are simply hashed and stored in the database to be compared with the password entered by the user. **NOTE** CCC stores passwords for local users only. CCC does not store passwords for the users imported from a Directory.
Device passwords	Each managed device uses two passwords, as follows: > When you add a device, you supply the device administrator password, which is used by CCC to log in to the Thales Luna Network HSM appliance. The device administrator password is encrypted (using a key stored in the root-of-trust HSM) and stored in the database. > When you authorize a device, you supply the HSM SO (Admin) password, which is used to authorize CCC to log in to the device as the HSM SO, using the root-of-trust HSM credentials. The HSM SO password is not stored in the database.
Root of trust partition password	While performing CCC activation, if you check the Remember credentials checkbox, the label and password of the root of trust partition will be cached in the JVM context. The root of trust partition password will be cached after applying the AES GCM Encryption algorithm on the password provided by the user. When the user deactivates a root of trust partition that was activated by checking the Remember credentials checkbox, the label and password of root of trust partition are unbound from the JVM context. When the CCC service shuts down, the cached root of trust label and password details get erased.

Modes of Operation

CCC provides the following two modes of operation:

Deactivated	In this mode, root-of-trust authentication is disabled, and CCC operates in read-only mode. > Administrator users cannot view users, organizations, devices or service. > Application Owner users can view the services created for their organization and download the CCC Client, but they cannot use the CCC Client to deploy the services.
Activated	In this mode, root-of-trust authentication is enabled, and all of the functions provided by CCC and the CCC Client are available.

You can activate and deactivate CCC as required. For enhanced security, you can choose to activate CCC only during specified HSM maintenance windows, if desired.

Root-of-Trust Authentication

All communications between CCC and the device HSMs are secured by the root-of-trust HSM. When you first activate CCC, a public/private key pair is generated on the root-of-trust HSM. When you authorize a device, the public key is copied from the root-of-trust HSM to the device HSM. This enables CCC to log in to the device as

the HSM SO, using the root-of-trust HSM credentials. Thereafter, any message sent from CCC to the device HSM is authenticated by signing the message with the private key on the root-of-trust HSM, and then verifying the message with the public key when it is received by the device HSM.

CHAPTER 2:
Setting up a CCC Server

This chapter describes the steps involved in setting up a CCC server. It contains the following sections:

Hardware and Software Requirements

For setting up a CCC server, you must have root level access to a Linux machine that meets the following hardware and software requirements:

Hardware Requirements

CPU	Quad Core, 2 GHz+
RAM	4 GB+
Free Disk Space	30 GB, if you are using a local PostgreSQL database **NOTE** Database space requirements are dependent on the number of HSM devices that CCC server is monitoring. Each device can accumulate up to 850 MB of data over a three-month period. If you are using the Monitoring feature, you would need an additional 20 MB on each partition over a 90-day period.

Operating System

64-bit CentOS	7, 8
64-bit RHEL	7, 8

> **NOTE** If you are using CentOS 8 or RHEL 8, ensure that the SELinux status is set to **permissive** or **disabled**. For this you need to open the /etc/selinux/config file and set the SELinux status to **permissive** or **disabled**. Reboot your system after saving the file.

JDK

During installation, JDK will be automatically installed on your machine. In case you want to use JDK that is already installed on your machine, you'll be asked to provide the installation path.

> **NOTE** CCC can use any version of Oracle JDK 1.8 or Open JDK 1.8, except 1.8-b144.

Database

PostgreSQL 9.5 **PostgreSQL 9.6** **PostgreSQL 10**	CCC installer detects the presence of PostgreSQL irrespective of the version and if does not find any database on the machine, then it prompts for installation of PostgreSQL 10.
Oracle 11g **Oracle 12c Release 1 (12.1)** **Oracle 12c Release 2 (12.2)**	It is recommended that your organization employ a trained Oracle Database Administrator (DBA) to configure a CCC Oracle database. To complete the configuration, the DBA needs to follow the instructions contained in the Installing Oracle Database section.

Root of Trust HSM

CCC supports the following HSM devices:

Thales Luna Network HSM	6.2.2 with firmware 6.24.9, 6.24.3, and 6.24.7 (recommended for FIPS compliance) 6.3 with firmware 6.24.7 (recommended for FIPS compliance) and 6.27.0 7.0 and 7.1 with firmware 7.0.1, 7.0.2, 7.1.0, 7.2, 7.3, and 7.3.3 (recommended for FIPS compliance)

Managed Devices

The HSM devices managed by CCC must meet the following requirements:

Model	Thales Luna Network HSM
Appliance Software	6.2.2, 6.3 Up to 7.3, 7.4 (FM disabled for full CCC features), 7.4 (FM enabled for device monitoring only) > **NOTE** Devices require REST API.

REST API for 6.x and 7.0 devices	7.1.0 - 7.1.0-380 7.2.0 - 7.2.0-221 7.3.0 - 7.3.0-166 7.4.0 - 7.4.0-228 **NOTE** REST API 7.0 is required for PUM and Apply/Support catalog features.
REST API for 7.1 devices	REST API is pre-installed on 7.1 devices and requires configuration
Firmware	6.24.7 or higher for 6.x devices Up to 7.3-165
Backup	Cloning or Key Export
Authentication	PED-authenticated or password authenticated. PED-authenticated devices must support remote PED

Luna HSM Clients

Luna HSM client version 6.2.2, 6.3, 7.0, 7.1, 7.2, 7.3, and 7.4 including the LunaJCPROV software. The root-of-trust HSM you use determines the type of Luna HSM client you require.

NOTE Luna HSM client version 7.4 is backward compatible with only 7.x devices.

Requirements for CCC Features

CCC Feature	Requires Monitoring License	Minimum SA Version	Minimum SA Firmware	Lunaclient
Service Provisioning		6.x	6.10.9	7.x
Security Officer Per Partition (PPSO)		6.x	6.10.9	7.x
Secure Trusted Channel (STC)		6.2.1	6.10.9	7.x
Device & Service Reports		6.x	-	7.x
Import Services		6.x	-	7.x
Device Monitoring, Dashboard & Notifications	Yes	6.x	6.10.9	7.x
Device Monitoring (Full)	Yes	6.x	6.20.0	7.x
Service Monitoring	Yes	7.3	7.3.0	7.x
Device Logs	Yes	6.x		7.x
Key Export		6.x	6.10.9	7.1 or above
Active Directory Support		NA	NA	
Apply SW Package		7.3	N/A	7.x
Update Firmware		7.3	N/A	7.x

Supported Browsers

CCC supports the latest versions of the following web browsers:

- Microsoft Edge
- Google Chrome

> Mozilla Firefox

When you are ready with a Linux machine that meets the hardware and software requirements for CCC, the next step involves Creating a Root of Trust.

Creating a Root of Trust

For setting up a CCC server, you need to create a root of trust (ROT) on an HSM device. Creating an ROT will allow the CCC to log into the HSM device as the Security Officer (SO) and will encrypt and decrypt all communications between the CCC and the managed devices. To create an ROT:

1. Log in as a root user on the Linux machine that you want to use for setting up a CCC server.
2. Install Thales Luna Network HSM Client software on this machine, ensuring that you've selected JCPROV from the list of components to be installed.
3. Log in to your Thales Luna Network HSM device and create a partition that will function as the ROT.
4. Create an NTLS between your device and the CCC server and then assign the ROT partition to the CCC server.

> **NOTE** To learn how to create an NTLS connection, refer the Thales Luna Network HSM documentation.

After you have created an ROT, the next step involves Installing CCC.

Installing CCC

After Creating a Root of Trust, follow these steps to install the CCC server, while ensuring that you are logged in as a root user:

1. **Downloading the CCC license file:**
   a. Log in to Thales Group Licensing Portal, using the details provided in the entitlement email you have received.
   b. Activate your CCC license and then download the license file.

> **NOTE** A Freemium license file is included in the CCC package that you'll be downloading in the next step. For more information about the different types of CCC licenses, click here.

2. **Downloading the CCC package:**
   a. Log in to the Thales Customer Support Portal and download the CCC package on to the CCC server.
   b. Unzip the CCC package and then go to the directory containing the RPM file and installation script.
3. **Checking installation requirements:**
   a. Run the `sh install.sh -check` command to check whether your system meets all the requirements for installing CCC.

b. If your system meets the hardware and software requirements, you will see a message stating that your system meets all the requirements, following which you can type **proceed** to begin the installation process.

c. If your system does not meet the hardware or software requirements needed for installing CCC, there are two possibilities:

- You'll see one or more warning messages indicating the missing components, following which you can either continue with the installation process or install the missing components first and then resume the installation process by running the `sh install.sh -check` command again.
- The installation process will get terminated due to errors and you will not be able to proceed further.

> **NOTE** You'll be asked to provide appropriate inputs at various stage of the installation process. The default inputs have been indicated by way of square brackets, wherever applicable. In case you press **Enter** without providing an input, the default inputs will be considered for the purpose of installation.

4. **Setting umask:** You will see a message indicating that umask has been set to **0022**.
5. **Installing CCC RPM:** The Crypto Command Center RPM package will be installed on your system.

> **NOTE** If a Crypto Command Center RPM package is already installed on your system, you'll be asked whether you want to uninstall and then reinstall the package.

6. **Installing JDK:** Java will be installed on your system. You'll be asked whether you wish to provide the path of an already installed JDK. If not, JDK be installed from the Web.
7. **Installing a database:** Specify the database that you want to use.

a. If you press **1**, you'll be asked whether you wish to install PostgreSQL locally or on an external server.

- If you opt for installing PostgreSQL locally, the installer checks for any existing version of PostgreSQL on your machine. If an existing version is found, it is offered to you for reconfiguration. If an existing version is not found, you need to specify whether you want to do the PostgreSQL installation through the Internet or via a local directory. Depending on your choice, PostgreSQL gets installed on your machine. After PostgreSQL has been installed, complete the rest of the installation process, as explained in steps 8 to 12 below.
- If you opt for installing PostgreSQL on an external server, you need to refer to the Installing PostgreSQL on an External Server section of the *CCC User Guide* for detailed steps. After you've installed PostgreSQL on an external server, you need to configure CCC, as described in the Configuring CCC section. You can skip the rest of the steps on this page.

b. If you select **2**, you need to install Oracle database on your system, as described in the Installing an Oracle Database section of this guide. After installing Oracle, you need to configure CCC, as described in Configuring CCC section. You can skip the rest of the steps on this page.

> **NOTE** To install Oracle, it is recommended that you should consult a trained Oracle Database Administrator (DBA). The DBA must refer the instructions provided in the Installing an Oracle Database section.

8. **Providing PostgreSQL listen address:** After you've installed PostgreSQL locally, you'll be asked to provide PostgreSQL listen address, which could either be a hostname or IP address. We recommend that you should provide **127.0.0.1** as the PostgreSQL listen address to identify the server in all configuration files. Unlike a hostname, **127.0.0.1** can be used in all the files.
9. **Configuring syslog:** Specify whether you want to configure syslog for PostgreSQL database logs.
10. **Configuring SSL:** You need to specify whether you want to configure PostgreSQL with SSL. If you choose **Yes**, you'll be asked to provide SSL Certificate details in step 12 below. If you choose **No**, step 12 will not be applicable to you.
11. **Creating database password:** You need to create a database password.
12. **Creating a self-signed certificate:** If you are configuring PosgreSQL with SSL, you need to create a self-signed certificate that will enable secure communication between the CCC server and PostgreSQL database. To do so, you need to specify your hostname, name of the organization unit, name of the organization, name of your city, name of your state or province, your 2-letter country code, and your email address.

After you've installed CCC, you need to change your current directory to /usr/safenet/ccc and initiate the CCC configuration process, as explained in the Configuring CCC section.

Configuring CCC

After Installing CCC, follow these steps to configure CCC:

1. **Checking configuration requirements:**
   a. Run the `sh config.sh -check` command from the **/usr/safenet/ccc** directory.
   b. If the server meets the configuration-related prerequisites, you will see a message stating that your system meets all the requirements, following which you can type **proceed** to begin the configuration process.
   c. If the server does not meet the configuration-related prerequisites, you will see a warning indicating the missing requirements. After you've made the required changes, you need to run the `sh config.sh -check` command again. If all the configuration-related requirements are met this time, you can type **proceed** to begin the configuration process.

> **NOTE** You'll be asked to provide appropriate inputs at various stage of the configuration process. The default inputs have been indicated by way of square brackets, wherever applicable. In case you press **Enter** without providing an input, the default inputs will be considered for the purpose of configuration.

2. **Checking CCC server state:** A check is conducted to determine whether the CCC server is running. In case the CCC server is running, you'll be asked to stop it before proceeding further.
3. **Setting umask:** You will see a message indicating that umask has been set to **0022**.
4. **Configuring JDK:** You'll be asked whether you want to change the JDK used by Crypto Command Center. In case you want to change the JDK, you need to provide the path.

5. **Configuring JCPROV:** You will see a message indicating the JCPROV has been configured. CCC server uses JCPROV APIs to access root of trust partition. For more information on JCPROV, refer to *Luna HSM User Guide*.
6. **Configuring firewall:** Specify whether you want to open the port used by CCC in the firewall.
7. **Configuring hosts file:**A check is conducted to ensure that the IP address and the hostname are mapped in the hosts file.
8. **Configuring SSL server certificates:** You need to decide whether you want to set an IP address in the subjectAltName of the SSL certificate. Following this, you need to create a Distinguished Name (DN) to include in your certificate request.

   > **NOTE** If no entry is provided for subjectAltName, then the entry provided for the distinguished name (DN) in the next step (host name/IP address) will be used for host attribute while deploying ccc_client.jar.

9. **Configuring keystores:** You'll be asked to change the vault, keystore, and truststore passwords.

   > **NOTE** **Truststore password** is used to access truststore contents. Truststore stores PostgreSQL or Oracle SSL certificates. **Keystore password** is used to access the keystore contents. Keystore holds the server certificate and private key. Whenever a client connects to the CCC server, the CCC server sends the certificate stored in the keystore to the client for verification. The client then verifies the certificate and begins communication with the CCC server.**Vault password** is used to access vault contents. Vault holds the truststore and keystore passwords.

10. **Configuring database:** Specify the database. Press **1** for PostgreSQL or **2** for Oracle.

    If you press **1** for PostgreSQL, you need to:

    a. Provide the database server's hostname or IP address. The default IP address is **127.0.0.1**.
    b. Specify whether you wish to configure CCC with PostgreSQL over SSL. The default option is **Yes**.
    c. Enter the database server's port number. The default port number is **5432**.
    d. Enter the database password.
    e. Enter the truststore password.

    If you press **2** for Oracle, you need to:

    a. Provide the database server's hostname or IP address.
    b. Specify whether you wish to configure CCC with Oracle over SSL. The default option is **Yes**.
    c. Enter the database server's port number. The default port number is **2484**.
    d. Enter the database server's service name.
    e. Enter the database password for Lunadirector user.
    f. Enter the database password for Keycloak user.
    g. Enter the truststore password.

11. **Completing CCC configuration:**

a. Enter **1**, **2**, or **3**, depending on whether you want to view the certificate, or import the certificate into the trusted keystore, or exit the configuration process.

b. After you've imported the certificate into the trusted keystore, you need to provide the vault password. At this point, the license persistence information will get initialized and the process of configuring CCC will get completed.

You can now log in to the CCC using the URL **https://<CCC Sever IP or hostname>:8181/**.

If you want to log in to the CCC server using the IP address, proceed to the Logging Into the Server section for the next steps.

If you want to log in to the CCC server using the hostname, you need to edit the hosts file to map your hostname to the IP address and then proceed to the Logging Into the Server section for the next steps. Follow these steps to map your hostname (for example, ccc) to the IP address (for example, 1.2.3.4):

> **Windows:** If you are a Windows user, go to C:\Windows\System32\drivers\etc\hosts, open the hosts file using a text editor, and add the following line: **1.2.3.4 ccc**.

> **Linux:** If you are a Linux user, go to /etc/hosts, open the hosts file using a text editor, and add the following line: **1.2.3.4 ccc**.

Now you can proceed to the Logging Into the Server section for the next steps.

Using a CA-Signed Certificate

If you do not sign the CCC SSL certificate using a trusted certificate authority (CA), the browser will warn the users that the connection is not trusted when they connect to the CCC server. To avoid this issue, you must have the certificate signed by a trusted CA. Alternatively, you can sign the certificate using a local CA, and import the local CA's certificate into the CCC server's keystore and into each user's browser. To use a CA-signed certificate

1. Log in to the CCC server workstation as root.
2. Enter the following command to set the umask to 0022:

   umask 0022
3. Go to the directory that contains the SSL certificates:

   cd /usr/safenet/ccc/cert
4. Create a copy of the certificate signing request (**.csr**) file with a file name that specifies the IP address or hostname that will be used to connect to the CCC server or server cluster.

   cp server.csr <ccc_hostname_or_IP>**.csr**

   For example:

   ```
   cp server.csr  my_ccc_server.csr
   ```
5. Transfer the <ccc_hostname_or_IP>**.csr** file to a Certificate Authority (CA) to sign it. You can transfer the file using scp, USB drive, email, etc.
6. Copy the signed certificate file to the **/usr/safenet/ccc/cert** directory.
7. Import the signed certificate to the trusted keystore.

cd /usr/safenet/ccc/cert
export CERT_PATH=/usr/safenet/ccc/server/standalone/configuration
export ALIAS=s1as

8. If you are using an untrusted local CA, import the CA certificate for the untrusted local CA to the CCC server. Otherwise, proceed to the next step:

   keytool -import -keystore $CERT_PATH/keystore.jks -alias <CA_alias> **-file** <filename>

   > **NOTE** The <CA_alias> is an arbitrary string of your choosing. Do not use **s1as** from the preceding step as the <CA_alias> string.

   Enter the keystore password when prompted.

9. Import the new signed certificate to the keystore:

   keytool -importcert-keystore $CERT_PATH/keystore.jks-alias $ALIAS -file <cert_filename>

   Enter the keystore password when prompted.

10. Restart the CCC service:

    systemctl restart ccc

11. If you are using an untrusted local CA, import the CA certificate for the untrusted local CA for each browser that will be used to access the CCC server. Otherwise, proceed to the next step.

12. Log in to the CCC server. You should be able to log in without the browser warning that the connection is not trusted.

Installing PostgreSQL on an External Server

To install PostgreSQL database on external server:

1. Add the hostname/IP of the database server to the CCC server's **/etc/hosts** file.
2. Download and install the PostgreSQL RPM.
3. Initialize the database.
4. Configure PostgreSQL to use syslog, if desired.
5. Configure the PostgreSQL listen address.
6. Configure PostgreSQL to use SSL.
7. Configure PostgreSQL to allow CCC to connect to the database.
8. Create the CCC database and user.

To add the external database server to the CCC server hosts file

1. Open the **/etc/hosts** file in a text editor.
2. Add an entry for the database server host. For example, the following entry adds the host **postgresql_server** at IP address 123.45.67.8:

   ```
   123.45.67.8 postgresql_server
   ```

3. Save and close the file.

Download and Install PostgreSQL

The PostgreSQL RPM is available for download from **postgresql.org**.

To download and install PostgreSQL

> **NOTE** As a CCC administrator, you can also install PostgreSQL during server installation. Please skip steps (1-5) mentioned below if you have decided to install PostgreSQL Database during server installation.

> **NOTE** As an example, all the following commands use PostgreSQL 10.

1. Log in as root to the server you will use to host the CCC PostgreSQL database.
2. Open a web browser and access the url: **http://yum.postgresql.org**.
3. Locate the correct PostgreSQL Yum Repository RPM for your operating system and copy its link location (URL). If you are using CentOS 8 or RHEL 8, run the `dnf -qy module disable postgresql &> /dev/null` command.
4. Enter the following command to install the RPM:

   yum install <rpm_url>

   If you are a CentOS 7 or RHEL 7 user, download PostgreSQL using the following link: https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm.

   If you are a CentOS 8 or RHEL 8 user, download PostgreSQL using the following link: https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm.
5. Install the PostgreSQL server.

   ```
   yum install postgresql10-server
   ```

Initialize the PostgreSQL Database and Start the PostgreSQL Service

You must initialize and start the database server before you can configure it for use with CCC.

1. Enter the following command to initialize the PostgreSQL database:

   ```
   /usr/pgsql-10/bin/postgresql-10-setup initdb
   ```
2. Enter the following command to enable automatic startup of the PostgreSQL database:

   ```
   systemctl enable postgresql-10.service
   ```

   Instructions for CentOS 8 and RHEL 8 users:

   If you are using CentOS 8 or RHEL 8, edit the service unit file of PostgreSQL from /usr/lib/systemd/system/postgresql-10.service and make the following entry in the [Unit] section:

   ```
   After=network-online.target
   ```

   Then save the file and run the following command:

   ```
   systemctl daemon-reload
   ```
3. Enter the following command to start the Postgresql service:

```
systemctl start postgresql-10
```

4. Open the /var/lib/pgsql/10/data/postgresql.conf file in a text editor and uncomment the following line:

   port = 5432

Configure PostgreSQL to Use Syslog (optional)

You can optionally configure PostgreSQL to send its logs to the syslog service. Using syslog is recommended.

1. Open the **/var/lib/pgsql/10/data/postgresql.conf** file in a text editor, and uncomment and configure the following lines in the **Error Reporting and Logging** section as indicated:
   - **log_destination = 'syslog'**
   - **syslog_facility = 'LOCAL0'**
   - **syslog_ident = 'postgres'**
2. Open the **/etc/rsyslog.conf** file in a text editor, and add the following line:

   local0.info /var/log/postgres
3. Enter the following command to restart the syslog or rsyslog service:

   systemctl restart rsyslog.service
4. Enter the following command to restart the PostgreSQL service:

   systemctl restart postgresql-10

Configure the PostgreSQL Listen Address

The **listen_addresses** setting specifies the TCP/IP address(es) of the IP interfaces that the PostgreSQL server listens on for connections from client applications. The **listen_addresses** setting controls which interfaces attempts to access the database, and should be configured such that connections are accepted only on the interfaces CCC uses to access the PostgreSQL database, to mitigate the risk of repeated malicious connection requests on insecure network interfaces. Refer to the PostgreSQL documentation for more information.

To configure the PostgreSQL listen address

1. Open the **/var/lib/pgsql/10/data/postgresql.conf** file in a text editor, and update the **listen_addresses =** setting in the **Connections and Authentication** section as follows:
   - If you are using an external database (standalone or HA), use the IP address or host name of the network interface CCC will use to connect to the database. You specify this IP address or host name when you run the CCC configuration script. See Configuring CCC for more information. For example, if the hostname of the PostgreSQL server is **ccc_db**, set the listen address as follows:

     listen_addresses ='ccc_db'

Enable PostgreSQL to Use SSL

CCC uses SSL to connect to the database. You must enable PostgreSQL to use SSL.

To enable PostgreSQL to use SSL

Open the **/var/lib/pgsql/10/data/postgresql.conf** file in a text editor, and uncomment and configure the **ssl =** setting in the **Connections and Authentication** section as follows:

ssl=on

Generate the SSL Key and Certificate

You must configure SSL and generate the SSL key and certificate used to authenticate the SSL connection. You must generate the key and certificate in the

/var/lib/pgsql/10/data directory. To generate the SSL key and certificate:

1. Go to the **/var/lib/pgsql/10/data** directory:

   cd /var/lib/pgsql/10/data

2. Enter the following commands to create a self-signed certificate with the correct permissions (644).

   openssl req -new -text -out server.req -nodes

3. Enter a passphrase, and respond to the prompts for country code, state or province, locality name, organization name, organizational unit, common name, and email address. Optionally enter a challenge password and company name. The key is generated. For the common name (CN), use the IP address or hostname which you configured as the PostgreSQL **listen-address**. You must also use the same IP address or hostname when you are prompted to enter the database server's hostname or IP address when configuring CCC.

4. To complete the registration of the SSL key enter the following commands:

   openssl rsa -in privkey.pem -out server.key

   rm -f privkey.pem

   openssl req -x509 -in server.req -text -key server.key -out server.crt

   chmod og-rwx server.key

   chown postgres:postgres server.req

   chown postgres:postgres server.crt

   chown postgres:postgres server.key

   systemctl restart postgresql-10.service

Configuring PostgreSQL to Allow Connections from CCC

To allow CCC to connect to the database, you must configure PostgreSQL to specify the location of the CCC server or HA cluster, the name of the database it is able to connect to (**lunadirectordb**), and the user name that it uses to connect (**lunadirector**).

To configure PostgreSQL to allow CCC to connect to the database

1. Open the **/var/lib/pgsql/10/data/pg_hba.conf** file in a text editor and add an entry for CCC to the **#IPv4 local connections** section of the file.

> **NOTE** To ensure that CCC can successfully connect to the database, the entry must be the first line in the **#IPv4 local connections** section.

Add the following line as the first entry in the section to allow connections from the CCC host:

hostssl lunadirectordb lunadirector <CCC_hostname_or_IP>/<mask> **md5**

For example, if your CCC host name is **ccc_server**, add the following line as the first entry in the section:

hostssl lunadirectordb lunadirector ccc_server md5

2. Save and close the file.
3. Restart the PostgreSQL service.

   systemctl restart postgresql-10.service

Creating the CCC Database and User

You must now create the database (**lunadirectordb**) and the user (**lunadirector**) that is allowed to access the database.

To create the lunadirectordb database and lunadirector user

1. Enter the following commands to create the **lunadirector** user and password, where <password> is the password the **lunadirector** user will use to access the database.

   > **NOTE** The password cannot contain a single quote (‘) or backslash (\) character.

2. Enter the following command to become the **postgres** superuser:

   su - postgres

   The bash shell prompt (**bash-4.1$**) is displayed.
3. Enter the following command to start **psql**:

   bash-4.1$ **psql**

   The **postgres=#** prompt is displayed.
4. Enter the following command to create the lunadirector user and password:

   postgres=# **create user lunadirector encrypted PASSWORD '**<password>**';**

   Postgres returns **CREATE ROLE**.

   For example:

   postgres=# **create user lunadirector encrypted PASSWORD 'CCCPa$$w0rd';**
   CREATE ROLE
5. Enter the following command to create the **lunadirectordb** database and assign ownership of the database to the **lunadirector** user:

   postgres=# **create database lunadirectordb owner lunadirector;**

   Postgres returns **CREATE DATABASE**.
6. Press **CTRL-D** to exit **psql.**

7. Enter **exit** to exit the postgres session.

> **NOTE** Remember the password you specified for the **lunadirector** user. You will need it later when you configure CCC.

Testing Your PostgreSQL Configuration

Installing and configuring PostgeSQL is complex and error prone. Before proceeding, test your PostgreSQL configuration to ensure that it is working correctly.

To test your PostgreSQL configuration

1. Ensure that you are logged in as root.
2. Enter the following command to become the **postgres** superuser:

   su - postgres

   The bash shell prompt (**bash-4.1$**) is displayed.
3. Enter the following command to test your PostgreSQL configuration:

   bash-4.1$ **psql "sslmode=require host=**<hostname> **dbname=lunadirectordb user=lunadirector"**

   where <hostname> is the hostname you configured in the **pg_hba.conf** file in "Configuring PostgreSQL to Allow Connections from CCC" on page 36

   If PostgreSQL is configured properly, you are prompted to enter the password for the **lunadirector** user (see "Creating the CCC Database and User" on the previous page). After successfully entering the password, the **lunadirectordb=>** prompt is displayed. If it is not, proceed to the next step to repair your configuration.
4. If the **lunadirectordb=>** prompt is not displayed, PostgreSQL is not configured correctly. Repeat or verify the following procedures:
   - "Enable PostgreSQL to Use SSL" on page 35
   - "Generate the SSL Key and Certificate" on page 36
   - "Configuring PostgreSQL to Allow Connections from CCC" on page 36

Viewing the PostgreSQL Server Logs

You can view the PostgreSQL server logs to audit database activity or to troubleshoot configuration issues. The logs are stored in the **/var/log/postgres** directory on the PostgreSQL server.

Installing Oracle Database

> **CAUTION!** CCC does not encrypt the contents of the database. Database encryption is supported by using an Oracle Server with tablespace encryption enabled through TDE.

You can configure CCC to store its data on an Oracle database instance. Oracle supports Transparent Data Encryption (TDE) on a tablespace.

It is recommended that your organization employ a trained Oracle Database Administrator (DBA) to complete the configuration of a CCC Oracle database.

> See the *Oracle Database Administrator's Guide* for more information about configuring and managing an Oracle database.

> See the *Oracle Database Security Guide* for more information about Oracle database security and user authentication.

> See the*Oracle Database Advanced Security Guide* for more information about configuring an Oracle database with TDE.

CCC Oracle Database Parameters for Oracle DBA

The following section contains recommendations for structuring and configuring an Oracle database for integration with CCC. We recommend you transfer this information to your Oracle DBA and request that the Oracle DBA configures a database for use with CCC based on these parameters.

Database size	850 MB per HSM device managed by CCC **NOTE** If you are using the Monitoring feature, you would need an additional 20 MB on each partition over a 90-day period.
Tablespace size	850 MB per HSM device managed by CCC **NOTE** If you are using the Monitoring feature, you would need an additional 20 MB on each partition over a 90-day period.
Projected growth for the database	Each device can accumulate approximately 850 MB of data over a 3 month period. Contact the Thales Group Customer Support portal for further information about reducing growth on the database. **NOTE** If you are using the Monitoring feature, you would need an additional 20 MB on each partition over a 90-day period.
Users	> lunadirector > keycloak See "Oracle Database Users" on the next page for a complete list of the necessary privileges for the database roles.
Service Name	Identifier for CCC database service. A service name can be associated with one or more SIDs. It allows the user to access multiple instances using the SERVICE_NAME identifier. See "Configure a Unique Service Name " on page 41 for more information about configuring a service name for your Oracle database. **NOTE** The CCC **config.sh** will prompt you for this information.
Oracle Wallet	Auto-login wallet Encryption wallet (optional, required for TDE)

TDE algorithm for tablespace encryption	The default algorithm for Oracle tablespace encryption is AES128. We recommend choosing an encryption algorithm that is compliant with your Corporate security policy.
Maximum number of connections to the database	20

Oracle Database Users

CCC requires the configuration of two users, lunadirector and keycloak, to communicate with the Oracle database. The two users require access to the same tablespaces. The lunadirector user and keycloak user passwords are required when you run the CCC server configuration script.

Review *Create User* in the *Oracle Database SQL Language Reference* for more information about creating Oracle database users.

The CCC Oracle database must have the following users:

User	Role
lunadirector	CCC user schema
keycloak	CCC authenticator

To create Oracle database users

1. Enter the following commands in sqlplus

   CREATE user lunadirector identified by <lunadirector_password> **default tablespace** <tablespace_name> **quota unlimited on** <tablespace_name> **;**

   CREATE user keycloak identified by <keycloak_password> **default tablespace** <tablespace_name> **quota unlimited on** <tablespace_name> **;**

   > **NOTE** The schema names are the same as the user names. The lunadirector user uses the lunadirector schema, and the keycloak user uses the keycloak schema.

The CCC Oracle database users must have the following privileges:

User	Privileges

lunadirector	`GRANT CREATE SEQUENCE to lunadirector;`
	`GRANT CREATE SESSION to lunadirector;`
	`GRANT CREATE TABLE to lunadirector;`
	`GRANT CREATE VIEW to lunadirector;`
	`GRANT CREATE PROCEDURE to lunadirector;`
	`GRANT CREATE TRIGGER to lunadirector;`

User	Privileges

keycloak	`GRANT CREATE SEQUENCE to keycloak;`
	`GRANT CREATE SESSION to keycloak;`
	`GRANT CREATE TABLE to keycloak;`
	`GRANT CREATE VIEW to keycloak;`
	`GRANT CREATE PROCEDURE to keycloak;`
	`GRANT CREATE TRIGGER to keycloak;`

> **NOTE** On Oracle databases the CCC uninstall script does not delete the lunadirector or keycloak user. The CCC uninstall script provides the option to drop all objects related to the lunadirector and keycloak users stored on the Oracle database. Inform your Oracle DBA that the users need to be dropped following the removal of CCC from the system.

Configure a Unique Service Name

You must decide on a unique service name for your CCC Oracle database instance. The service name is required when you run the CCC **config.sh** script.

Review section 2.8.1 of the *Oracle Database Administrator's Guide* for more information about configuring a service name for your database instance.

Oracle Wallets

CCC uses SSL to communicate with the database, so you must create an Oracle wallet with an SSL certificate. To enable tablespace encryption through TDE you require an encryption wallet.

When the **config.sh** script is run the Oracle certificate is transferred to the CCC trust store. When CCC communicates with the Oracle server it compares the Oracle certificate with the certificate stored in the CCC trust store.

See *Using Oracle Wallet Manager* for more information about Oracle Wallets.

To create an Oracle Auto-login Wallet

You must create an Oracle wallet to securely store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL in the Oracle database.

1. Log into the Oracle database and create a wallet directory.

   mkdir u01/app/oracle/wallet

2. Create an auto-login wallet.

   orapki wallet create -wallet "u01/app/oracle/wallet" -pwd <wallet_password> -**auto_login_local**

3. Generate a self-signed certificate and load it into the wallet.

   orapki wallet add -wallet "/u01/app/oracle/wallet" -dn "CN=oracle,O=<company>**C=**<country>**" -keysize 2048 -self_signed -validity 7300 -pwd** <wallet_password> **-sign_alg sha256 -nologo**

4. Open the **sqlnet.ora** file in a text editor. The file is located at **$ORACLE_HOME/network/admin/sqlnet.ora**. Alter the information so it appears as the following:

```
WALLET_LOCATION =
  (SOURCE =
  (METHOD = FILE)
```

```
  (METHOD_DATA =
  (DIRECTORY = /u01/app/oracle/wallet)
  )
 )
SQLNET.AUTHENTICATION_SERVICES = (TCPS,NTS,BEQ)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_
AES_128_CBC_SHA256)
```

5. Open the **tnsnames.ora** file in a text editor. The file is located at **$ORACLE_HOME/network/admin/tnsnames.ora**. Alter the information so it appears as the following:

```
<tnsname>=
 (DESCRIPTION=
  (ADDRESS=
  (PROTOCOL=TCPS)
  (HOST=0.0.0.0)
  (PORT=2484)
 )
 (CONNECT_DATA=
 (SERVER=dedicated)
 (SERVICE_NAME=CCC)
 )
)
```

6. Open the **listener.ora** file in a text editor. The file is located at **$ORACLE_HOME/network/admin/listener.ora**. Alter the information so it appears as the following:

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION =
 (SOURCE =
 (METHOD = FILE)
  (METHOD_DATA =
  (DIRECTORY = /u01/app/oracle/wallet)
  )
 )
LISTENER =
 (DESCRIPTION_LIST =
  (DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = oracle)(PORT = 1521))
  (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
  (ADDRESS = (PROTOCOL = TCPS)(HOST = oracle)(PORT = 2484))
  )
 )
TRACE_LEVEL_LISTENER = 4
TRACE_FILE_LISTENER = listener.trc
```

7. Check the status of **lnsrctl** by running the command **lnsrctl status**. If the wallet is configured properly the command will complete successfully.

```
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oracle)(PORT=1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=oracle)(PORT=2484)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=oracle)(PORT=5500))(Security=(my_wallet_
directory=/u01/app/oracle/<wallet>))(Presentation=HTTP)(Session=RAW))
Services Summary...
Service "CCC" has 1 instance(s).
Instance "CCC", status READY, has 1 handler(s) for this service...
Service "CCCXDB" has 1 instance(s).
```

```
Instance "CCC", status READY, has 1 handler(s) for this service...
The command completed successfully
```

To create an encryption wallet

For creating an encryption wallet to enable tablespace encryption through TDE on an Oracle database:.

1. Log onto the Oracle database as the oracle user.
2. Create an encryption wallet directory:

   mkdir /u01/app/oracle/encryption_wallet
3. Open the **sqlnet.ora** file in a text editor and add the new section **ENCRYPTION_WALLET_LOCATION** section to point to the encryption wallet directory.

   > **NOTE** The **ENCRYPTION_WALLET_LOCATION** information should be made in addition to the **WALLET_LOCATION** section of the **sqlnet.ora** file.

   The **sqlnet.ora** file is available at **/u01/app/oracle/product/**<product_version>**/dbhome_1/network/admin**. Add the following information to the **sqlnet.ora** file.

   ```
   ENCRYPTION_WALLET_LOCATION=
   (SOURCE=
   (METHOD=FILE)
   (METHOD_DATA =
   (DIRECTORY= /u01/app/oracle/encryption_wallet)))
   ```
4. Create the wallet and assign a wallet password:

   orapki wallet create -wallet /u01/app/oracle/encryption_wallet -pwd <encryption_wallet_password>

   This will create an **ewallet.p12** file in the **encryption_wallet** directory.

Oracle TDE Example Procedural Sets

The following procedural sets are sample documentation on enabling tablespace encryption through TDE on a CCC Oracle Database. These Oracle databases were configured using the SQLPlus command line interface and the Oracle DBCA tool. They provide information about the process of configuring an Oracle database with tablespace encryption enabled through TDE.

> **NOTE** Access to the TDE software keystore will allow the user full access to the database.

See the *Oracle Database Advanced Security Guide* for more information about configuring an Oracle database with TDE.

Configuring an Oracle Database with TDE (Optionally: to be used by CCC)

You can configure an Oracle database with tablespace encryption enabled through TDE to support CCC. You create the Oracle database and run the CCC **config.sh** server configuration script. The following objects and users must exist to configure an Oracle database with tablespace encryption to support CCC:

> a running database instance

- ORACLE_SID environment variable set to SID for database instance
- Oracle Advanced Security

To enable TDE the Oracle user must have access to:

- ADMIN privileges
- Oracle wallet
- Encryption wallet

To configure an Oracle database with TDE to be used by CCC

1. Log in to the database as the database administrator and create the encrypted tablespace.

   sqlplus / as sysdba

   a. Generate the master encryption key:

      ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY <encryption_wallet_password> **;**

   b. Create an encrypted tablespace:

      CREATE TABLESPACE <tablespace_name> **DATAFILE /u01/app/oracle/oradata/**<database_instance>**/datafile/**<database_file>**SIZE 200M AUTOEXTEND ON NEXT 20M ENCRYPTION USING AES128 DEFAULT STORAGE (ENCRYPT) ;**

   c. Check if the tablespace was encrypted:

      SELECT TABLESPACE_NAME, ENCRYPTED FROM DBA_TABLESPACES ;

      The command returns:

```
TABLESPACE_NAME                    ENC
---------------------------------------
SYSTEM                              NO
<Tablespace Name>                  YES
```

2. Create the lunadirector user and grant the user privileges.

   a. Create the lunadirector user and set the default tablespace:

      CREATE user lunadirector IDENTIFIED BY <lunadirector_password>
      DEFAULT TABLESPACE <tablespace_name> **QUOTA UNLIMITED ON** <tablespace_name> **;**

      Now, when tables are created for the lunadirector user they will be created in the encrypted tablespace.

   b. Grant the lunadirector user privileges.

      GRANT CREATE SEQUENCE to lunadirector**;**

      GRANT CREATE SESSION to lunadirector**;**

      GRANT CREATE TABLE to lunadirector**;**

      GRANT CREATE VIEW to lunadirector**;**

      GRANT CREATE PROCEDURE to lunadirector**;**

      GRANT CREATE TRIGGER to lunadirector**;**

3. Create the keycloak user and grant the user privileges:

   a. Create the keycloak user and set the default tablespace:

CREATE user keycloakIDENTIFIED BY <keycloak_
password> **DEFAULT TABLESPACE** <tablespacename>
QUOTA UNLIMITED ON <tablespacename> **;**

Now, when tables are created for the keycloak user they will be created in the encrypted tablespace.

b. Grant the keycloak user privileges:

GRANT CREATE SEQUENCE to keycloak**;**

GRANT CREATE SESSION to keycloak**;**

GRANT CREATE TABLE to keycloak**;**

GRANT CREATE VIEW to keycloak**;**

GRANT CREATE PROCEDURE to keycloak**;**

GRANT CREATE TRIGGER to keycloak**;**

4. Run the CCC **config.sh** script.

Enabling Tablespace Encryption on an Oracle Database for an Existing CCC Installation

You can migrate your existing CCC Oracle database to an Oracle database with tablespace encryption. The following objects and users must exist to enable TDE for CCC on the Oracle database:

- Oracle database
- Oracle Advanced Security
- lunadirector user
- keycloak user

To enable TDE the Oracle user must have access to:

- ADMIN privileges
- Oracle Wallet
- Encryption Wallet

To enable tablespace encryption on an Oracle database for an existing CCC installation

1. Stop your CCC server.

   service ccc stop

2. Log into the Oracle Database as Oracle user.
3. Export the Oracle data directory:

   a. In sqlplus create a directory to export the data to.

   create directory <dump_directory> **as '/u01/app/oracle/admin/**<database_instance>**/dpdump/';**

   b. From a server console as the Oracle user, export the entire <tablespace_name> to the dump directory.

   expdp userid="'/ as sysdba"' dumpfile=<dumpfile_name> **directory=**<dump_directory> **logfile=**<tablespace_logfile>**tablespaces=**<tablespace_name>

   <dumpfile>**.dmp** should now be visible in the **/u01/app/oracle/admin/**<database_instance>**/dpdump/** directory.

4. Take a backup of your database.
5. Log into sqlplus and print out the command that created the tablespace.

   SELECT dmbs_metadata.get_ddl('TABLESPACE', '<tablespace_name>**') FROM DUAL;**

   The following is an example of the commands output:

```
CREATE TABLESPACE "<tablespace_name>" DATAFILE
'/u01/app/oracle/oradata/<database_instance>/datafile/<database_file>.dbf' SIZE 20971520
AUTOEXTEND ON NEXT 8192 MAXSIZE 32767M
LOGGING ONLINE PERMANENT BLOCKSIZE 8192
EXTENT MANAGEMENT LOCAL AUTOALLOCATE DEFAULT
NOCOMPRESS  SEGMENT SPACE MANAGEMENT AUTO
```

   Copy the output as you will need to edit it in sqlplus at a later stage.
6. Remove the existing tablespace.
   a. In sqlplus take the existing tablespace offline.

      alter tablespace<tablespace_name> **offline;**

   b. In sqlplus drop the tablespace and delete the data files.

      Drop tablespace <tablespace_name> **including contents and datafiles;**

   c. From a Linux command prompt confirm that your data files no longer exists on the tablespace. The following command will fail if the data files were removed.

      ls -l /u01/app/oracle/oradata/<database_instance>**/datafile/**<database_file>**.dbf**
7. Edit the create tablespace command output from step 5 to add encryption.
   a. Take the output from the **SELECT dmbs_metadata.get** command and remove the following:

```
PERMANENT
DEFAULT
NOCOMPRESS
```

      NOTE In our configuration we had to remove these values. Your results may vary.

   b. Add the following information as the final line of the CREATE TABLESPACE command.

```
ENCRYPTION using 'AES256' DEFAULT STORAGE (ENCRYPT)
```

   c. Create your tablespace and the **.dbf** file. In sqlplus run the new CREATE TABLESPACE command.

      CREATE TABLESPACE "<tablespace_name>**" DATAFILE**

      '/u01/app/oracle/oradata/<database_instance>**/datafile/**<database_file>**.dbf' SIZE 20971520**

      AUTOEXTEND ON NEXT 8192 MAXSIZE 32767M

      LOGGING ONLINE BLOCKSIZE 8192

      EXTENT MANAGEMENT LOCAL AUTOALLOCATE

      SEGMENT SPACE MANAGEMENT AUTO

      ENCRYPTION using 'AES256' DEFAULT STORAGE (ENCRYPT);

> **NOTE** Enabling encryption on a tablespace results in a full table update like any ALTER TABLE command.

d. From a Linux command prompt import the <tablespace> file you created earlier.

impdp userid="'/ as sysdba'" dumpfile=<tablespacedump_file> **directory=**<dump_directory> **logfile=**<tablespace_logfile> **tablespaces=**<tablespace_name>

e. In sqlplus confirm you can see any tables associated with your users.

select table_name from dba_tables where owner = 'LUNADIRECTOR';

select table_name from dba_tables where owner = 'KEYCLOAK';

f. Confirm that users are associated with the correct tablespace.

select * from dba_users where username in ('LUNADIRECTOR', 'KEYCLOAK');

```
DEFAULT_TABLESPACE
------------------------------
USERS
USERS
```

8. In sqlplus confirm that the tablespace was encrypted.

SELECT TABLESPACE_NAME,ENCRYPTED FROM DBA_TABLESPACES where TABLESPACE_NAME = '<tabespace_name>**';**

If the tablespace is properly encrypted, the commands output will be the following:

```
TABLESPACE_NAME              ENC
-------------------------------
<tablespace_name>             YES
```

9. Restart the CCC Service.

service ccc start

High-Availability Configurations

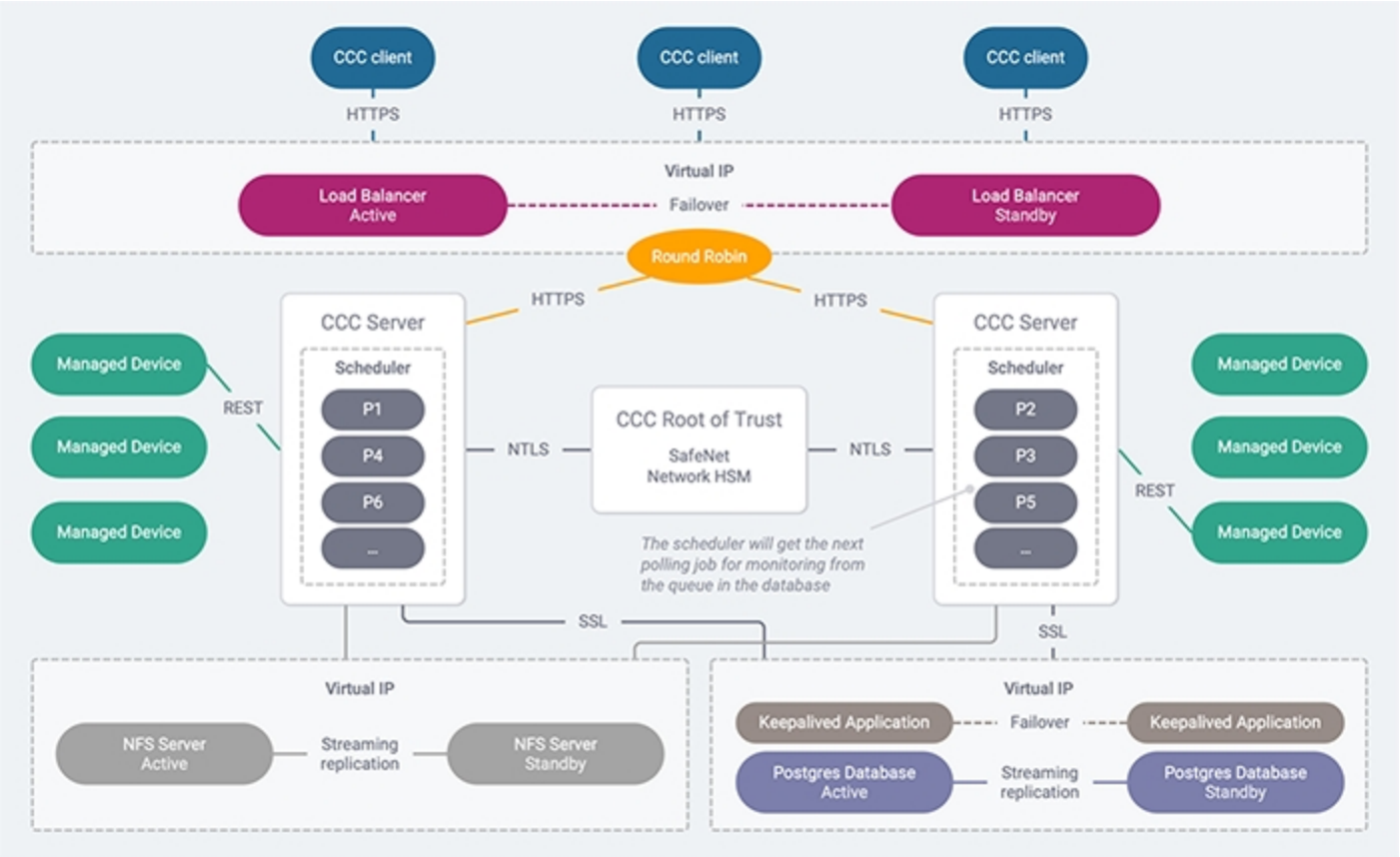
This section describes a sample configuration for deploying CCC in a high availability configuration. CCC provides an open and flexible architecture that supports multiple configuration options, including high availability. By adding additional and standby components to the basic configuration you can create a high availability system that offers the following features:

- Server redundancy
- Load balancing
- Data replication
- Failover protection

Deployment Architecture for CCC High Availability Setup

Here's an illustration of a CCC configuration that provides all of the features inherent in a high-availability system.

Figure 5: Example of a High Availability Configuration



Server Redundancy

A true high-availability system needs to continue to operate, without interruption, in the event that one of the system components fails. To deliver this capability, it is recommended that you set up two CCC servers, two PostgreSQL database servers, two NFS servers, and two load balancers, with the load balancer sending requests to the CCC servers in a round-robin fashion.

Although you can configure your system to use a single load balancer, it is recommended that you deploy standby load balancers to avoid having a single point of failure. If you plan on using standby load balancer servers, you need to configure the servers to use a single virtual IP address and to provide automatic failover in the event of a server outage.

> **NOTE** If you wish to configure standby Oracle databases, please consult Oracle documentation.

Load balancing

The load balancers are installed on a separate server, and sit between the CCC clients and CCC server. When clients connect to CCC, they do so by pointing to the IP address/host name of the load balancer. The load balancer takes each request in order and routes it to one of the CCC servers. If one of the CCC servers goes down, the request is forwarded to the next server, with no impact to the end user. The load balancer must be configured to support persistent (or sticky) sessions, such that all requests for a specific user session are directed to the same CCC server. If a failover occurs, the user will be prompted to log in to another active server, and all future requests will be directed to the new server for the duration of the session.

Data replication

It is recommend that you configure PostgreSQL or Oracle database to provide streaming replication of the database between an active and standby database server. Any HA implementation should include this, or a similar feature, to ensure uninterrupted access to the data stored in the CCC database in the event of a failure.

It is recommended that you configure NFS server to provide streaming replication of CCC data between the active and standby NFS servers. Any HA implementation should include this, or a similar feature, to ensure uninterrupted access to the data stored on the NFS server in the event of a failure.

Failover protection

You can configure each of the standby components to provide failover.

Load balancers typically allow you to configure a virtual IP address for the server cluster, with one active server and one standby server. The servers communicate with each other using a keepalive mechanism. The virtual IP address is used by the active server, which accepts all client requests and routes them to the CCC servers in a round-robin fashion (or similar method, depending on how you configured your load balancer). If the active server goes down, the standby server takes the IP address and becomes the active server.

Database failover is managed by installing an application, such as keepalived, on each database server that allows you to use a virtual IP address to identify the active database server so that if the active server goes down, the standby server takes the IP address and becomes the active server. Notification of a failover is also required so that the databases can be re-synchronized when the failed database server is brought back online.

NFS server failover is managed by installing an application, such as keepalived, on each NFS server that allows you to use a virtual IP address to identify the active NFS server so that if the active server goes down, the standby server takes the IP address and becomes the active server.

> **NOTE** Operations that are in progress when a failover occurs may fail.

Deploying CCC in HA Configuration

To deploy CCC in HA configuration and set up file sharing among CCC servers, follow these steps on each NFS server:

1. Run the **enableNFSSharing.sh** script on the NFS server that you've selected. This script will be available at the path **/usr/safenet/ccc/scripts/enableNFSSharing.sh** on a CCC server. Copy this script from the CCC server to NFS server. Following is the general command syntax for executing the enableNFSSharing.sh script:

   ```
   ./enableNFSSharing  <NFSOption>  <IPAddress(s)>
   ```

   > **NOTE** Values allowed for `<NFSOption>` are: **1** for NFS Server and **2** for NFS Client.

   > **NOTE** If you execute the `enableNFSSharing.sh` script without any arguments or wrong arguments, you will get the following message: “Usage: enableNFSSharing NFSOption[1: For NFS Server 2: For NFS Client] IPAddress”.

   > **NOTE** Enter valid IP addresses to avoid getting an error.

2. Run the following command on the NFS server by navigating to the folder where **enableNFSSharing.sh** script is copied :

   `./enableNFSSharing.sh 1` <List of all the CCC servers to be setup in HA mode as NFS client, separated by a space>

   Example:

   ```
   ./enableNFSSharing.sh 1 20.10.10.10 30.10.10.10
   ```

3. Run the following script on CCC servers to set up the NFS client:

   ```
   ./enableNFSSharing.sh 2 <IP of NFS Server/Virtual IP of NFS server cluster in case CCC is set up in high availability>
   ./enableNFSSharing.sh 2 10.10.10.10
   ```

To Unmount NFS Dir during CCC Uninstall

1. To unmount NFS directory during uninstall, CCC administrator runs following command as 'root' user:

   umount -f -l /usr/safenet/ccc/packages

   > **NOTE**
   > 1. This step should be performed only if CCC is set up in HA mode.
   > 2. This step should be performed on all CCC servers that have been set up as NFS client.

Tested Configuration

This section describes how to set up the HA configuration which was validated by the engineering team.

HAProxy load balancer

This is a Linux server that accepts the client requests and routes them to one of the active CCC servers in the cluster. You require HAProxy 1.5 or higher.

> **NOTE** This tested procedure demonstrates setting up a single load balancer, instead of the recommended redundant configuration because of the wide variety of possible implementations. With a single load balancer, you will lose connectivity in the event of a server outage, although this will not affect the integrity of the data stored in CCC. You may wish to consult HAProxy documentation to set up two load balancers in active-standby mode.

Redundant CCC application servers

The CCC application is installed on two separate CentOS 7 workstations that receive requests from the load balancer. Requests are sent to the individual CCC servers from the load balancer in a round-robin fashion, so that if one of the servers goes down, the request is forwarded to the next available server. In addition, you must configure HAProxy to use "sticky sessions", so that once a client logs in using a certain CCC server, all further requests from that client session will be sent to the same CCC server.

> **NOTE** While this example considers CentOS 7, the scenario is also valid for CentOS 8, RHEL 7, and RHEL 8.

PostgreSQL servers

PostgreSQL is installed on two separate Linux workstations and is configured to use streaming replication. Keepalived is installed on each database server to provide failover and notification.

High-Level Procedure

Deploying CCC in a high-availability configuration involves performing the following tasks:

1. Install the operating system and configure the network on each server required for the HA configuration, as described in "Server OS Installation and Network Configuration" on the next page.
2. Install and configure the primary and standby PostgreSQL database servers, as described in "To Configure and Setup PostgreSQL Server in HA Mode " on page 53. This involves performing the following tasks:
   a. Installing PostgreSQL on each database server.
   b. Configuring the primary and standby database servers and enabling streaming replication.
   c. Testing streaming replication.
   d. Installing and configuring keepalived on the primary and standby database servers.
   e. Testing keepalived.
3. Install and configure primary and standby NFS servers, as described in "Deploying CCC in HA Configuration " on the previous page. This involves performing the following tasks:
   a. Installing NFS Utilities on each NFS server.

   b. Configuring the primary and standby NFS servers and enabling streaming replication.
   c. Testing streaming replication.
   d. Installing and configuring keepalived on the primary and standby NFS servers.
   e. Testing keepalived.
4. Set up and configure the CCC servers, as described in "CCC Application Server Setup and Configuration" on page 61. This involves performing the following tasks:
   a. Installing and initializing a Thales Luna Network HSM partition to serve as the CCC root-of-trust HSM for both CCC servers.
   b. Installing the CCC application server software on each CCC server.
   c. Running the CCC server configuration script (**config.sh**) on each CCC server.
5. Set up and configure the HAProxy server to act as a load balancer for the CCC servers, as described in "HAProxy Server Setup and Configuration" on page 61.

Server OS Installation and Network Configuration

An HA deployment requires seven separate servers which exchange data with each other, over the network, to operate as a unified system. When you configure CCC in HA, you are required to specify the network address (IP address or host name) of specific servers in the deployment. To simplify the deployment and avoid potential misconfigurations, the first step in deploying an HA configuration is to perform the following tasks:

> install the operating system on each server used in the deployment.

> configure the IP address or host name that will be used to identify the server.

> assign a role to each server.

> **NOTE** You must reserve two additional IP addresses - one for the database cluster and the other one for the NFS cluster. These IP addresses need to be specified during database configuration.

This document uses variables to identify each of the servers in the deployment, as listed in the following table. After you complete the OS installation and network configuration, record the IP address or host name of each server on the following table, so that you can easily refer to this information when performing the various configuration tasks.

Server	Alias	IP address/Host name
Primary (active) PostgreSQL server	<db_primary_IP_or_hostname>	
Standby PostgreSQL server	<db_standby_IP_or_hostname>	
Keepalived database cluster virtual IP address	<keepalived_virtual_IP>	
Primary (active) NFS server	<nfs_primary_IP_or_hostname>	

Server	Alias	IP address/Host name
Standby NFS server	<nfs_standby_IP_or_ hostname>	
Keepalived nfs cluster virtual IP address	<keepalived_virtual_IP>	
CCC server 1	<ccc1_IP_or_hostname>	
CCC server 2	<ccc2_IP_or_hostname>	
HAProxy load balancer	<ha_proxy_IP_or_hostname>	

To install the OS and configure the network settings

Perform the following procedure on each server that will be used in the HA deployment:

1. Install the CentOS 7 distribution for your server architecture:
   a. CentOS 7 is available for download from http://wiki.centos.org/Download. It is recommended that you install only the base software (the **Minimal** installation option) to avoid installing unnecessary software that could present a security risk. Refer to the CentOS documentation for detailed installation instructions.
   b. After the installation is complete, reboot the system by entering the command **systemctl reboot**.
   c. Log in as root and enter the **yum update** command to install the latest updates.
2. Configure a static IP address or host name on the server and record the information in the table above. Refer to the CentOS documentation for detailed network configuration procedures.

To Configure and Setup PostgreSQL Server in HA Mode

This section describes how to set up a PostgreSQL high availability (HA) cluster configuration consisting of a primary PostgreSQL server and a standby PostgreSQL server. The cluster is configured to use streaming replication. This procedure assumes PostgreSQL 10.

Refer to the PostgreSQL documentation at https://www.postgresql.org/docs/10/index.html for more information.

Installing PostgreSQL

You require two standalone Linux servers: one for the primary, and one for the standby. The tested and documented configuration uses CentOS 7 and PostgreSQL 10. Other operating systems may work, although they are not tested, and may use different paths for some components. To install PostgreSQL on an external server, refer to the Installing PostgreSQL on an External Server section.

Configuring the Primary PostgreSQL Database Server

This section describes how to perform the following tasks on the primary PostgreSQL database server:

> configure PostgreSQL to use streaming replication

- allow the standby PostgreSQL server and each CCC application server to access the primary PostgreSQL server
- create an SSL certificate to authenticate the connection between the CCC servers and the database
- create the database tables and users
- configure the firewall to provide access to the port used by the database

To configure the primary PostgreSQL database server

1. Log in as root to the server you identified as the primary PostgreSQL server and set the permissions for the session:

   su root

   umask 0022

2. Edit the **/var/lib/pgsql/10/data/postgresql.conf** file to uncomment and update the following entries, which are used to configure PostgreSQL to use streaming replication:

   listen_addresses = '<db_primary_IP_or_hostname>,<keepalived_virtual_IP>**'**
   ssl = on
   wal_level = hot_standby
   checkpoint_segments = 32
   archive_mode = on
   archive_command = 'cp %p /tmp/%f'
   max_wal_senders = 3
   wal_keep_segments = 32

   > **NOTE** **listen_addresses** is a comma separated list of the hosts the server will respond to. It must also include the keepalived virtual IP address for the database cluster (configured later), and may include other servers, if required. Access to the database is controlled by the **pga_hba.conf** file (next step).

3. Open the **/var/lib/pgsql/10/data/pg_hba.conf** file in a text editor and add an entry for CCC to the **#IPv4 local connections** section of the file. Add the following lines as the first entry in the section to allow connections from the CCC host:

   > **NOTE** To ensure that CCC can successfully connect to the database, the entry must be the first lines in **#IPv4 local connections** section.

   host replication replicator <db_secondary_IP_or_hostname>**/32 md5**

   hostssl lunadirectordb lunadirector <ccc1_IP_or_hostname>**/32 md5**

   hostssl lunadirectordb lunadirector <ccc2_IP_or_hostname>**/32 md5**

   > **NOTE** If both of your CCC servers reside in the same subnet, you can add a single line to the file to allow access from all devices in that subnet. Add an entry for **hostssl lunadirectordb lunadirector** <subnet_IP>**/24 md5** as the last line in the **var/lib/pgsql/10/data/pg_hba.conf** file.

4. Save and close the file.
5. Restart the PostgreSQL Service.

   systemctl restart postgresql-10.service
6. The connection between the CCC application servers and the PostgreSQL servers uses SSL, which requires that you create a server certificate. Enter the following commands to create a self-signed certificate with the correct owner and permissions.

   After entering the **openssl req -new -text -out server.req -nodes** command, you will be presented with a series of prompts asking you to specify the certificate attributes. The only important attribute is the server **Common Name (CN)**, which must be set to the virtual IP of the database cluster, which is configured in "Setting Up Keepalived On the PostgreSQL Servers" on page 58. You must specify the virtual IP, since the same certificate will be used on the standby database server to handle failover.

   cd /var/lib/pgsql/10/data

   openssl req -new -text -out server.req -nodes

   openssl rsa -in privkey.pem -out server.key

   rm -f privkey.pem

   openssl req -x509 -in server.req -text -key server.key -out server.crt

   chmod og-rwx server.key

   chown postgres:postgres server.key

   systemctl restart postgresql-10
7. Enter the following commands to set up the replication and CCC users and tables in the database:

   su - postgres -c "psql postgres postgres -c \"CREATE USER replicator REPLICATION LOGIN PASSWORD 'dbpass';\""

   su - postgres -c "psql postgres postgres -c \"CREATE USER lunadirector encrypted PASSWORD '<password>**';\""**

   where <password> is the password the **lunadirector** user will use to access the database.

   > **NOTE** Remember the password you specified for the lunadirector user. You will need it later when you configure CCC. This is the password that the CCC application server uses to connect to the PostgreSQL database cluster.

   su - postgres -c "psql postgres postgres -c \"CREATE DATABASE lunadirectordb OWNER lunadirector;\""
8. Enter the following command to configure the firewall (iptables) to allow the CCC servers to access the database. By default, PostgreSQL listens on port 5432 for connections:

   iptables -I INPUT 2 -p tcp -m tcp --dport 5432 -j ACCEPT

Configuring the Standby PostgreSQL Database Server

This section describes how to perform the following tasks on the standby PostgreSQL database server:

> configure PostgreSQL to use streaming replication

- allow the standby PostgreSQL server and each CCC application server to access the primary PostgreSQL server
- copy the SSL certificate used to authenticate the connection between CCC servers and the database from the primary server
- copy the database tables and users from the primary server to the standby server
- configure the firewall to provide access to the port used by the database

To configure the standby PostgreSQL database server

1. Log in as root to the server you identified as the primary PostgreSQL server and set the permissions for the session:

   su root

   umask 0022

2. Edit the **/var/lib/pgsql/10/data/postgresql.conf** file to uncomment and update the following entries, which are used to configure PostgreSQL to use streaming replication:

   listen_addresses = '<db_standby_IP_or_hostname>,<keepalived_virtual_IP>**'**
   ssl = on
   wal_level = hot_standby
   checkpoint_segments = 32
   max_wal_senders = 3
   wal_keep_segments = 32
   hot_standby = on

3. Open the **/var/lib/pgsql/10/data/pg_hba.conf** file in a text editor and add an entry for CCC to the **#IPv4 local connections** section of the file. Add the following lines as the first entry in the section to allow connections from the CCC host:

   > **NOTE** To ensure that CCC can successfully connect to the database, the entry must be the first lines in **#IPv4 local connections** section.

   host replication replicator <db_secondary_IP_or_hostname>**/32 md5**

   hostssl lunadirectordb lunadirector <ccc1_IP_or_hostname>**/32 md5**

   hostssl lunadirectordb lunadirector <ccc2_IP_or_hostname>**/32 md5**

   > **NOTE** If both of your CCC servers reside in the same subnet, you can add a single line to the file to allow access from all devices in that subnet. Add an entry for **hostssl lunadirectordb lunadirector** <subnet_IP>**/24 md5** as the last line in the **var/lib/pgsql/10/data/pg_hba.conf** file.

4. Save and close the file.
5. Restart the PostgreSQL Service.

   systemctl restart postgresql-10.service

6. Copy the database from the primary PostgreSQL server to the standby PostgreSQL server. Copying the database deletes the **/var/lib/pgsql/10/data** directory that contains the **postgresql.conf** configuration file, so the following step includes backing up the directory and restoring it after copying the database.

   a. Ensure that you are not in the **/var/lib/pgsql/10/data** directory:

      cd

   b. Backup the PostgreSQL configuration files:

      cp /var/lib/pgsql/10/data/postgresql.conf /tmp/postgresql.conf.bak

      cp /var/lib/pgsql/10/data/pg_hba.conf /tmp/pg_hba.conf.bak

   c. Stop the PostgreSQL service:

      systemctl stop postgresql-10

   d. Delete the /var/lib/pgsql/10/data/ directory. It will be restored later.

      sudo -u postgres rm -rf /var/lib/pgsql/10/data/

   e. Replicate the database from the primary database server to the standby database server:

      sudo -u postgres pg_basebackup -h <db_primary_IP_or_hostname> **-D /var/lib/pgsql/10/data -U replicator -v -P**

      where <db_primary_IP_or_hostname> is the IP address of host name of the primary database server.

      You are prompted to enter the password for the 'replicator' user. The password is 'dbpass', as configured in "Configuring the Primary PostgreSQL Database Server" on page 53.

      The following message may be displayed. It can be ignored.

      ```
      could not change directory to "/root": Permission denied
      ```

   f. Enter the following commands to configure the **recovery.conf** file:

      sudo -u postgres bash -c "cat > /var/lib/pgsql/10/data/recovery.conf <<- _EOF1_
      standby_mode = 'on'
      primary_conninfo = 'host=<db_primary_IP_or_hostname> **port=5432 user=replicator password=dbpass'**
      trigger_file = '/tmp/postgresql.trigger'
      EOF1
      "

   g. Restore the postgresql.conf and pg_hba.conf files from the backups:

      cp -f /tmp/postgresql.conf.bak /var/lib/pgsql/10/data/postgresql.conf

      cp -f /tmp/pg_hba.conf.bak /var/lib/pgsql/10/data/pg_hba.conf

   h. Start the PostgreSQL service:

      systemctl start postgresql-10

7. Enter the following command to configure the firewall (iptables) to allow the CCC servers to access the database. By default, PostgreSQL listens on port 5432 for connections:

   iptables -IINPUT 2 -p tcp -m tcp --dport 5432 -j ACCEPT

Testing the PostgreSQL Database Cluster

To verify that streaming replication is configured correctly, you can create a table on the primary database and verify that it is replicated on the standby database.

To test the PostgreSQL database cluster

1. Create a table (named **test**) on the primary database:

   su - postgres -c "psql postgres postgres -c \"CREATE TABLE test (name char(10));\""

2. Verify that the table was replicated on the standby database:

   a. Login to the standby database server as root:

      su root

   b. Start PostgreSQL.

      systemctl start postgresql-10

   c. Connect to the database:

      su - postgres

      psql -d postgres

   d. List the tables in the database:

      \dt *.*

      If streaming replication is configured correctly, the **test** database table is listed in the output. If it is not, check your configuration and try again.

3. Delete the table (named **test**) on the primary database:

   su - postgres -c "psql postgres postgres -c \"DROP TABLE test;\""

4. Attempt to create a table (named **test**) on the standby database:

   su - postgres -c "psql postgres postgres -c \"CREATE TABLE test (name char(10));\""

5. Verify that the command fails with the following error:

   ```
   "ERROR:  cannot execute CREATE TABLE in a read-only transaction"
   ```

Setting Up Keepalived On the PostgreSQL Servers

You must install the **keepalived** software on each PostgreSQL server to manage failover to the standby server in the event of an outage on the primary server. Once keepalived is installed and configured, if the primary server goes down, the standby server takes over as the new primary server, and the old primary server becomes the standby server. Keepalived allows you to configure a virtual IP address for the database cluster, so that database failover is transparent to CCC. For more information, refer to the keepalived documentation, available at keepalived.org.

To install and configure keepalived on the PostgreSQL database servers

1. Install keepalived on both of the PostgreSQL database servers:

   yum install keepalived

2. Edit the **/etc/keepalived/keepalived.conf** file on the primary server as follows, where:

<email_address>	The email address used to send a notification message in the event of a failover.
<smtp_server_IP_or_ hostname>	The IP address or hostname of the SMTP server used to send the notification message.
<db_cluster_virtual_IP>	The virtual IP address for the database cluster.
<eth0 | eth1 | eth2 | ...>	The interface to bind to the virtual IP address.You can use the current interface, or a different interface, if available. To determine the current interface, enter the command **ip addr**. Unless you want to use a different interface, you can use the current interface for both the **vrrp_instance** and **virtual_ipaddress** entries.

NOTE Replace all existing content so that your file contains only the following entries.

```
! Configuration File for keepalived

global_defs {
   notification_email {
   }
   notification_email_from <email_address>
  smtp_server <smtp_server_IP_or_hostname>
   smtp_connect_timeout 30
   router_id CCC_DB_MONITOR
}

vrrp_instance VI_1 {
   state MASTER
   interface <eth0 | eth1 | eth2 | ...>
   virtual_router_id 51
   priority 101
   advert_int 1
   authentication {
      auth_type PASS
      auth_pass PASSWORD
   }
   virtual_ipaddress {
     <db_cluster_virtual_IP> dev <eth0 | eth1 | eth2 | ...>
   }
}
```

3. Edit the **/etc/keepalived/keepalived.conf** file on the standby server as follows, where:

<email_address>	Specifies the email address used to send a notification message in the event of a failover.
<smtp_server_IP_or_hostname>	Specifies the IP address or hostname of the SMTP server used to send the notification message.

<db_cluster_virtual_IP>	Specifies the virtual IP address for the database cluster.
<eth0 | eth1 | eth2 | ...>	Specifies the network interface to bind to the virtual IP address. Choose the interface you want to use.
<path to notify_master script>	Specifies the path to the notify master server script. Deactivates the PostgreSQL service on the primary database server in event of failover.
<path to notify_backup script>	Specifies the path to the notify backup server script. Alerts the secondary database that the primary has failed and switches the server from read-only to active.

NOTE Replace all existing content so that your file contains only the following entries.

```
! Configuration File for keepalived

global_defs {
   notification_email {
   }
   notification_email_from <email_address>
  smtp_server <smtp_server_IP_or_hostname>
   smtp_connect_timeout 30
   router_id CCC_DB_MONITOR
}

vrrp_instance VI_1 {
   state BACKUP
   interface <eth0 | eth1 | eth2 | ...>
   virtual_router_id 51
   priority 100
   advert_int 1
   authentication {
      auth_type PASS
      auth_pass PASSWORD
   }e
   virtual_ipaddress {
    <db_cluster_virtual_IP> dev <eth0 | eth1 | eth2 | ...>
   }
   notify_master /root/<path to notify_master script>
   notify_backup /root/<path to notify_standby script>
}
```

4. Enter the following command on both of the PostgreSQL database servers to configure the firewall (iptables) to allow multicast:

   iptables -I INPUT -i eth2 -d 224.0.0.0/8 -j ACCEPT

5. Start keepalived on both of the PostgreSQL database servers, beginning with the primary:

   systemctl start keepalived

6. Restart postgresql on both of the PostgreSQL database servers, beginning with the primary:

systemctl restart postgresql-10

Testing keepalived

You can verify that keepalived is working by performing the following tasks on both database servers:

> view the logs in **/var/log/messages** .

> run the following command to see if the virtual IP is bound where you expect it to be. In normal operation, the virtual IP is bound to the primary database server only:

ip addr show <**eth0** | **eth1** | **eth2** | ...>

NFS Server Setup and Configuration

For detaled steps involved in NFS server setup and configuration, refer to "Deploying CCC in HA Configuration " on page 50.

CCC Application Server Setup and Configuration

Setting up and configuring the CCC application servers involves performing the following tasks on each server used to host the CCC application. Refer to the Setting up a CCC Server section for detailed procedures describing how to perform these tasks.

To set up and configure the CCC servers

1. Install and initialize the root-of-trust HSM, as described in Creating a Root of Trust. The root-of-trust HSM must be a Thales Luna Network HSM partition.
2. Install the CCC application server software. Refer to Installing CCC. You need to perform the following tasks:
   a. Install the Java JDK.
   b. Install the CCC server software.
3. Run the CCC server configuration script (**config.sh**) to configure the Crypto Command Center application server. Refer to Configuring CCC for a detailed procedure.
   - when creating the certificate signing request, you are prompted to enter the server common name. This is the address of the HAProxy server. If you specify an IP address, you will be warned of a mismatch between the server's actual IP address and the HAProxy IP address. To avoid this issue, use a fully qualified domain name for the HAProxy server.
   - when prompted for the IP address of the database server, enter the virtual IP address for the database cluster, as configured in "Setting Up Keepalived On the PostgreSQL Servers" on page 58. Both Crypto Command Center servers must point to the same virtual IP.

HAProxy Server Setup and Configuration

In an HA configuration, users connect to CCC through a server running the HAProxy load balancer. HAProxy accepts client requests and routes them to any of the active CCC servers in a round-robin fashion.

HAProxy is configured to use SSL in pass-through mode, which is supported in HAProxy 1.5 or higher only. In addition, you must configure HAProxy to use "sticky sessions", so that once a client logs in using a certain CCC server, all further requests from that client session will be sent to that same CCC server. Without sticky sessions, the client will be asked to log in again every time they are routed to a new CCC server.

To set up and configure the HAProxy server

> **NOTE** The following section describes a sample script for the **haproxy.cfg** file. The exact parameters of your **haproxy.cfg** file may be dependent on your systems requirements. It is recommended that you refer to the HAProxy documentation for more information on customizing the configuration file for your specific networks needs.

1. Install the CentOS distribution for your server architecture:
   a. CentOS is available for download from http://www.centos.org. It is recommended that you install only the base software (the **Minimal** installation option) to avoid installing unnecessary software that could present a security risk. Refer to the CentOS documentation for detailed installation instructions.
   b. After the installation is complete, reboot the system.
   c. Log in as root and enter the **yum update** command to install the latest updates.
2. Install HAProxy:
   a. Log in as root and set the permissions for the session:

      su root

      umask 0022

   b. Install HAProxy:

      yum install haproxy
3. Edit the **/etc/haproxy/haproxy.cfg** file to configure the HAProxy server:
   a. Update the "Main Frontend" section to replace the default entries with the following entries, which will instruct HAProxy to route incoming SSL connections on port 8181:

      frontend https-in
      mode tcp
      bind *:8181
      default_backend app

   b. Update the "Static Backend" section by commenting the following entries:

      # backend app

      # balance roundrobin

      # server static 127.0.0.1:4331 check

   c. Update the "Round-Robin Balancing" section to replace the default entries with the following entries, which enable sticky sessions and describe the CCC servers that will handle incoming requests:

      backend app
      mode tcp
      balance roundrobin
      stick-table type binary len 32 size 30k expire 30m

```
acl clienthello req_ssl_hello_type 1
acl serverhello rep_ssl_hello_type 2
tcp-request inspect-delay 5s
tcp-request content accept if clienthello
tcp-response content accept if serverhello
stick on payload_lv(43,1) if clienthello
stick store-response payload_lv(43,1) if serverhello
server ccc1 <ccc1_IP_or_hostname>:8181
server ccc2 <ccc2_IP_or_hostname>:8181
```

> **NOTE** Selinux should be set to permissive mode to achieve the intended results. If this is not permissible by your companies policy then you will need to make alterations to the **haproxy.cfg** file.

Many more options are available; see the HAProxy documentation for details about the specific requirements of your server and network configuration.

4. Enter the following command to allow connections to the HAProxy server on port 8181:

   iptables -A INPUT -p tcp --dport 8181 -m state --state NEW,ESTABLISHED -j ACCEPT

5. Restart the HAProxy service:

   systemctl restart haproxy

6. Verify that you can connect to CCC through the HAProxy server:

   https://<haproxy_server_ip_or_hostname>**:8181**

Add / Delete CORS Settings

This section describes how to add/delete CORS Settings in CCC to add or delete a domain in the PostgreSQL/Oracle database. It contains the following sections:

> "Adding/Deleting a CORS Domain in PostgreSQL" below

> "Adding/Deleting a CORS domain in Oracle " on the next page

Adding/Deleting a CORS Domain in PostgreSQL

The CCC Administrator can add and delete a CORS domain in PostgreSQL database by adding the CORS setting in the CCC.

To add a CORS domain in PostgreSQL

1. Go to the CCC installation directory:

   cd /usr/safenet/ccc

2. Launch the CORS configuration script:

   sh cors_manager.sh

3. Select **PostgreSQL**.

4. Enter the database **server's hostname** or **IP address**.

5. Enter the database server's **port number**.
6. Enter the database **password** for lunadirector user**.**
7. Enter the **Crypto Command Center server's trust store password**.

   When the trust store password is entered, the database connection is established successfully.
8. Select **To add CORS domain** as Operation Type.
9. Enter the domain. The domain is added successfully.

   The CCC administrator is prompted to add another domain.
10. Select **Y** if you want to add another domain or select **N** if you do not want to add another domain.

To delete a CORS domain in PostgreSQL

1. Go to the CCC installation directory:

   cd /usr/safenet/ccc
2. Launch the CORS configuration script:

   sh cors_manager.sh
3. Select **PostgreSQL**.
4. Enter the database **server's hostname** or **IP address**.
5. Enter the database server's **port number**.
6. Enter the database **password for** lunadirector user**.**
7. Enter the **Crypto Command Center server's trust store password**.

   When the trust store password is entered, the database connection is established successfully.
8. Select **To delete CORS domain** as Operation Type.
9. Enter the domain. The domain is deleted successfully.

   The CCC administrator is prompted to delete another domain.
10. Select **Y** if you want to add another domain or select **N** if you do not want to add another domain.

> ****WARNING**** The configuration script performs pattern matching. Ensure to enter the relevant domain name to perform the deletion operation successfully.

Adding/Deleting a CORS domain in Oracle

The CCC Administrator can add and delete a CORS domain in Oracle databse by adding the CORS setting in the CCC.

To add a CORS domain in Oracle

1. Go to the CCC installation directory:

   cd /usr/safenet/ccc
2. Launch the CORS configuration script:

   sh cors_manager.sh

3. Select **Oracle**.
4. Enter the database **server's hostname** or **IP address**.
5. Enter the database server's **port number**.
6. Enter the database server's **service name**.
7. Enter the database **password** for lunadirector user.
8. Enter the **Crypto Command Center server's trust store password**.

   When the trust store password is entered, the database connection is established successfully.
9. Select **To add CORS domain** as Operation Type.
10. Enter the domain. The domain is added successfully.

    The CCC administrator is prompted to add another domain.
11. Select **Y** if you want to add another domain or select **N** if you do not want to add another domain.

To delete a CORS domain in Oracle

1. Go to the CCC installation directory:

   cd /usr/safenet/ccc
2. Launch the CORS configuration script:

   sh cors_manager.sh
3. Select **Oracle**.
4. Enter the database **server's hostname** or **IP address**.
5. Enter the database server's **port number**.
6. Enter the database server's **service name**.
7. Enter the database **password** for lunadirector user.
8. Enter the **Crypto Command Center server's trust store password**.

   When the trust store password is entered, the database connection is established successfully.
9. Select **To delete CORS domain** as Operation Type.
10. Enter the domain. The domain is deleted successfully.

    The CCC administrator is prompted to delete another domain.
11. Select **Y** if you want to delete another domain or select **N** if you do not want to delete another domain.

> ****WARNING**** The configuration script performs pattern matching. Ensure to enter the relevant domain name to perform the deletion operation successfully.

> **NOTE** If the database connection is not established successfully while adding **CORS Settings** in **PostgreSQL / Oracle** database, the connection attempt failed error displays.

Upgrade

The following section contains recommendations for upgrading CCC. The section will detail guidelines for upgrading clients, devices, and databases for integration with CCC. It contains the following topics:

> "Upgrading CCC to use lunaclient 7.x" below

Upgrading CCC to use lunaclient 7.x

The recommended upgrade path is:

> install lunaclient 7.x

> install CCC 3.7.1

> **NOTE** For new installations of CCC we recommend that you install the lunaclient 7.x and then CCC. If the lunaclient 7.x is already installed when the 3.7.1 **config.sh** script is run then the lunadirector user will be included in the hsmusers group.

If the user upgrades their CCC and subsequently upgrades to use a 7.x lunaclient they must add the lunadirector user to the hsmusers group. This allows CCC to access the lunaclient information

> **NOTE** While upgrading CCC to the latest version, it is advised to upgrade JDK also to the latest version. For knowing the latest JDK version supported, refer to the Customer Release Notes (CRN).

To add lunadirector to the hsmusers groups

1. Log in as root
2. Add lunadirector to the hsmusers group

   sudo gpasswd --add lunadirector hsmusers

CHAPTER 3:
Administration

This chapter describes how to use the CCC administrative interface to manage users, devices, and services, generate reports, and perform server administration tasks. It contains the following sections:

Server Administration

This section describes how to perform server administration tasks. It contains the following sections:

Overview

CCC Administrator users are able to activate and deactivate the CCC root-of-trust HSM, as described in "Root of Trust Activation and Deactivation" on the next page. When the root of trust is disabled, CCC operates in view-only mode.

The CCC Administrator is responsible for managing licenses that are required to activate access to the CCC. Acquiring a license allows you to upgrade from a trial version to a full version, renew your license subscription, set the maximum provisioned partitions limit, or access the monitoring feature on HSM devices. See "Managing Licenses" on page 70.

The server Administrator can also start or stop the CCC service, outside of CCC, to enable or disable the CCC server, as described in "Managing the CCC Service" on page 72.

Regular backups are essential to allow you to successfully recover from a disaster. See "Backup and Restore" on page 73.

To help troubleshoot operational issues you may encounter, such as failure to connect to devices, or provision services, you can view the logs, as described in "Server Administration" on the previous page.

Logging Into the Server

Only users with the **Admin** role can log in to the CCC as an Administrator. By default, the **Admin** role has one user, the **admin** user. An active license is required for access, so if a license is absent, you are prompted to upload one on activation of the CCC.

To login to the server as an Administrator

1. Launch CCC using a supported browser (CCC supports the latest versions of Microsoft Edge, Google Chrome, and Mozilla Firefox browsers). The URL you use depends on whether the server is identified by IP address or hostname, as follows:
   - **https://**<host_ip>**:8181**
   - **https://**<hostname>**:8181**

   The **Crypto Command Center Login** page is displayed.
2. Login to the CCC as an admin user.

   If this is the first time you are logging into the server, use the following credentials:

User Name	admin
Password	PASSWORD

3. Change the password, if you are prompted.
4. Upload the license file from your local filesystem, if you are prompted.

   The license summary is displayed, indicating the license type affiliated with your CCC. You can later manage your licenses as described in "Managing Licenses" on page 70.

Root of Trust Activation and Deactivation

You can activate and deactivate the CCC server, as required, to limit its ability to log in to the managed devices. For example, you may want to limit periods of activation to specific maintenance windows, to reduce the risk of unauthorized activity in CCC.

Activating the Root of Trust

You need to activate the root of trust on first login to CCC, and to re-activate CCC any time it has been deactivated. You may also need to re-activate the root of trust if its address or credentials are changed.

> **NOTE** You must be able to see the root-of-trust HSM as a slot in your Luna client before you can activate it.

To activate the root of trust

1. Click on the **Administration** tab, and select **Activation** in the navigation frame to display the CCC Activation page.
2. Enter the **Partition label** and **Password**.
3. Check the **Remember credentials** checkbox if you want CCC to cache your root of trust credentials, and then click the **Activate** button.

> **NOTE** In case you don't want CCC to cache your root of trust credentials, you can leave the Remember credentials checkbox unchecked. When the CCC service is restarted, the root of trust label and password details get erased automatically.

Activating a New Root of Trust

To activate a new root of trust, you need to reauthorize all the devices managed in the CCC.

To activate a new root of trust

1. Restart the CCC server.
2. Enter the **Partition label** and **Password**.
3. Check the **Remember credentials** checkbox if you want CCC to cache your root of trust credentials, and then click the **Activate** button.
4. Click the **Devices** tab and select the device.
5. Open the **Connections** tab and then click the **Update Credentials** button.
6. Open the Authorization tab and then click the **Re-Authorize** button.

Deactivating the Root of Trust

You can deactivate the root of trust to prevent CCC from logging into the managed devices, or to prevent Application Owners from using the CCC Client (ccc_client) to deploy services.

To deactivate the root of trust

1. Click on the **Administration** tab, and select **Activation** in the navigation frame to display the CCC Activation page.
2. Click **Deactivate**.

Root of Trust Self Activation

To view the steps involved in automatic ROT activation, click here.

Managing Licenses

Access to CCC functionality is regulated by licenses. An active license is required to access the CCC graphical user interface. CCC must be activated to upload a license file. A single license can apply to multiple CCC instances in a high availability configuration.

Once the license expires, you are given a grace period during which you still have access to full CCC functionality. This grace period is to allow some time to order and obtain a new license file. Once the period ends, Administrators cannot import more partitions, create new services, or activate new services, and Application Owners cannot deploy existing services.

CCC users have access to the following license types:

Freemium	A Freemium license is included in the CCC software package and can be applied to the product once installed. The Freemium license provides access to 20 device partitions and can also enable the device monitoring feature. The Freemium license is deployed in a test environment and should not be used in a production environment.
Premium - Trial	The Premium - Trial license is a 90-day trial license distributed for assessment purposes. The number of device partitions that can be provisioned by the Premium - Trial license is specified in the license file, as per the license agreement. The Premium - Trial license can be deployed in a test or production environment. It can also enable the device monitoring feature.
Premium - Subscription	The Premium - Subscription license is an annual subscription-based license. The number of device partitions that can be provisioned by the Premium - Subscription license is specified in the license file, as per the license agreement. The Premium - Subscription license is deployed in a production environment. It can also enable the device monitoring feature.
Premium - Perpetual	The Premium - Perpetual license is a one-time purchase license. The number of device partitions that can be provisioned by the Premium - Perpetual license can is specified in the license file, as per the license agreement. The Premium - Perpetual license is for deployment in a production environment. It can also enable the device monitoring feature.

NOTE For more information about license types and acquiring your CCC License contact your Thales sales representative.

Upgrading the license allows you to upgrade from a trial version to a full version, renew your license subscription, or increase the maximum provisioned partitions limit.

> **NOTE** The CCC license files are set in the UTC time zone. As a result, the expiry dates on the individual license files may not coincide with your local time zone.

To view the license information

1. Click on the **Administration** tab, and select **Licenses** in the navigation frame.

   The following information is displayed:

License Type	The service level (Freemium or Premium) and duration of your license.
Features	Lists the features made available by the uploaded license. These features can include monitoring and provisioning.
Maximum Provisioned Partitions	The number of Thales Luna HSM partitions which you may manage through CCC.The Freemium License allows access to 20 fixed partitions. The entitlements of the Premium License will define the quantity of available partitions.
Partitions Used	The number of Thales Luna HSM partitions which are currently managed through CCC.
License Activation Date	The date when the license was activated in the Sentinel EMS portal.
License Expiration Date	The date when the license will expire. This date can be calculated relative to the activation date, as with a trial license, or can be fixed based on your license term. This field is displayed while CCC is still within its licensed period of operation. If the user has purchased a perpetual license this information is not displayed.

The following additional fields are displayed if you exceed the license limits by using an expired license, or managing more partitions than allowed:

License Grace Period Ends	The date when the grace period for the CCC license will expire, and functionality will be reduced. Once the period ends, Administrators cannot import more partitions, create or activate new services, and Application Owners cannot deploy existing services.

To upload a license

1. Click on the **Administration** tab, and select **Licenses** in the navigation frame.
2. Obtain the new license and place it in the local filesystem.

> **NOTE** Access the Thales Customer Support portal for more information about obtaining a license.

3. Click the **Upload License** button. The **Upload License** dialog is displayed.
4. Click the **Upload** button and select the new license file from your filesystem.

> **NOTE** The license type and entitlements are displayed in the **Update License** dialog.

5. Click the **Continue** or **Update** button.

To update a license

1. Click on the **Administration** tab, and select **Licenses** in the navigation frame.
2. Obtain the new license and place it in the local filesystem.

> **NOTE** Access the Thales Customer Support portal for more information about obtaining a license.

3. Click the **Update License** button. The **Update License** dialog is displayed.
4. Click the **Update...** button and select the new license file from your filesystem.

> **NOTE** The license type and entitlements are displayed in the **Update License** dialog.

5. Click the **Update** button.

> **NOTE** The **Update License** button is now enabled with Freemium license also. The CCC user can now apply a premium license to replace a Freemium license using this Upload License button as per the requirement.

Managing the CCC Service

The CCC web server runs as a service. The service must be running for the server to be available. You can use the following set of commands to manage the CCC service:

Command	Description
systemctl start ccc	Start the CCC service. The service must be running to use CCC.
systemctl stop ccc	Stop the CCC service. If you stop the service, CCC will not be available for use.
systemctl restart ccc	Restart the CCC service. This command stops and restarts the service.
systemctl status ccc	Display the current status of the CCC service.

To start, stop, restart, or display the status of the CCC service

1. Log in, as root, to the Linux server used to host the CCC server.
2. Enter a command from the list above, as desired.

Backup and Restore

Database and root-of-trust HSM backups are essential to allow you to successfully recover from a disaster.

Regular database backups are required. Refer to the *PostgreSQL* documentation or the *Oracle Database Backup and Recovery User Guide* for database backup and restore procedures.

Ensure that you backup the root-of-trust HSM after you first activate CCC. Refer to the *Thales Luna HSM* documentation for more information.

Root of Trust Self Activation

CCC can cache your root of trust partition label and password at the time of activation and use them later for reactivation in case of a network disruption. To Enable ROT Self Activation:

1. Click on the **Administration** tab, and select **Activation** from the navigation pane to display the CCC Activation page.

2. Enter the partition label and password.

3. Check the **Remember credentials** checkbox and then click the **Activate** button.

> **NOTE** In case you don't want CCC to cache your root of trust credentials, you can leave the Remember credentials checkbox unchecked.

External Directory Server Support over LDAP

The key highlights of External Directory Server Support over LDAP feature are as follows:

- As a CCC administrator, you can add any number of directories into the CCC server and then import, provision, and manage users from those directories.
- At the time of user creation, the CCC imports various details associated with the user into the database, such as the First Name, Last Name, User Name, and Email Address.
- The imported user can be assigned either the administrator role or application owner role.
- When a directory user tries to log in to the CCC application, the user authentication request is forwarded to the external directory associated with the user. After receiving a confirmation, the CCC performs user authorization to identify whether the user is an administrator or application owner.
- CCC provides a flexible directory sync service to either manually sync the configured directory for any changes or define a scheduled sync to manage the changes.
- CCC never stores user password details in case of directory users and provides support to Add External Directory over secured as well as unsecured communication channels.
- CCC can work with directory services over LDAP provided by any vendor, including Microsoft Active Directory, Microsoft Azure Directory, and Redhat Directory Service.
- In case a user leaves the organization and the user details are deleted from the directory server, the CCC server will sync the details as per the scheduled sync and update the records.
- As a CCC administrator, you can also perform manual sync on that directory server. Post sync, if that user tries to log in to the CCC server, the CCC server authentication will fail.

For further details, refer to Adding and Managing Directories.

Adding and Managing Directories

You can use the **Directories** tab to add, manage, and configure user directories that contain data about the CCC users and groups.

To use this feature, you need to log on to CCC as an administrator, click the **Administration** button from the menu bar at the top, followed by **Directories** tab from the left-side navigation pane. The **Directories** page that appears contains detailed information about the directories that are already configured in your CCC application.

For adding or configuring a new directory, click the **Add Directory** button and then provide the following details.

Field	***Explanation***
Directory Display Name	*Enter a name for the directory that you want to configure.*
Vendor	*Select an LDAP vendor.*

LDAP over SSL	*Check this option if you want to create a secure connection with the LDAP directory. Ensure you have imported an SSL certificate in the CCC server truststore before checking the check-box.*
	To import an SSL certificate in truststore, run the following command:
	`keytool -import -alias <unique_alias> -file <full path of cert file> -storetype JKS -keystore /usr/safenet/ccc/server/standalone/configuration/cacerts.jks -storepass <password>`
	To list all the SSL certificates you've imported, run the following command:
	`keytool -list -storetype JKS -keystore /usr/safenet/ccc/server/standalone/configuration/cacerts.jks`
	NOTE You need to restart the CCC server after importing the SSL certificate.

Connection URL	*Provide a connection URL to your LDAP server .* *(For example, <protocol ldap/ldaps>://<hostname/ip>:<port number>)*
Username LDAP Attribute	*Provide the name of LDAP attribute that is mapped as the CCC user name.*
RDN LDAP Attribute	*Provide the name of LDAP attribute that is used as Relative Distinguished Name (RDN).*
UUID LDAP Attribute	*Provide the name of LDAP attribute that is used as Unique Object Identifier (UUID).*
User First Name LDAP Attribute	*Provide the name of the mapped first name attribute on the LDAP object.*
User Last Name LDAP Attribute	*Provide the name of the mapped last name attribute on the LDAP object.*
User Email LDAP Attribute	*Provide the name of the mapped email address attribute on the LDAP object.*
User Object Classes	*Provide all values of LDAP objectClass attribute for users in LDAP separated by comma.*
Users DN	*Provide full Distinguished Name (DN) of LDAP tree where your users are.*
Authentication Type	*Select the LDAP Authentication Type. You can choose from None (anonymous LDAP authentication) or Simple (bind credential + bind password authentication) mechanisms.*
Bind DN	*Provide DN of LDAP admin that'll be used by CCC to access LDAP server.*
Bind Credential	*Provide password of LDAP admin.*

Custom User LDAP Filter (Optional)	*You have the option to provide an additional filter that you can use to filter searched users. Ensure that it begins with "(" and ends with ")".*
Search Scope	*You can use search scope options to select the level of search scope. Level One searches for users in DNs specified by user DNs. Subtree searches for users in the entire Subtree.*
Enable Users Sync	*You can enable Users Sync to perform synchronization of LDAP users to CCC at specified intervals. The minimum sync time is 10 minutes.*

Click the **Add Directory** button after you've entered the required inputs. You'll then be able to see the newly created directory on the **Directories** page. You can use this page for the following purposes:

- **Status:** You can use the Status column to validate the status of any directory. A green tick icon before the name of a directory indicates that it is Active. On the other hand, an orange error icon before the name of the directory indicates that it's Inactive.
- **Name:** You can find the names of all the directories associated with the CCC application in the Names column.
- **Connection URL:** You can validate connection information of each directory through the Connection URL column.
- **Next Sync:** In case you've used the **Enable Users Sync** option to automate syncing for a particular directory, that information will appear here.
- **Sync Users:** You can use the blue sync icon to sync one or more directories whenever required.
- **Last Sync Status:** This column will display the details regarding the last syncing, including its timing, status, number of users synced, number of users removed, and users that could not be synced.
- **Actions:** You can use the Actions column to edit the specifications of a directory or to delete a directory. If you are deleting a directory that you had configured over SSL, it's recommended that you also delete its corresponding SSL certificate from the CCC truststore using the following command:

```
keytool -delete -alias <certificate_alias> -keystore
/usr/safenet/ccc/server/standalone/configuration/cacerts.jks -storepass <password>
```

> **NOTE** You need to restart the CCC service after deleting the SSL certificate.

Account Management

This section describes how to perform user account management tasks. It includes the following topics:

- Types of Users in CCC
- Adding and Managing Users

Types of Users in CCC

There are two types of users in CCC:

- **Admin** users are able to access the Administrator Dashboard, add users and devices, create services, configure email notifications, and perform server administration tasks.

> **Application Owner** users are able to deploy services created by the CCC Administrator for the members of their organization. They can also see service monitoring statistics for their managed services. Individual Application Owners must belong to an organization. When you add an Application Owner user account, you must assign the user to an organization. The organization must exist prior to adding the user. The user and organization management functions are grouped under the **Accounts** tab.

The following table compares the capabilities of the CCC Admin and CCC Application Owner users:

Feature	CCC Admin	CCC Application Owner
Service Creation	Yes	No
Service Initialization	Yes	Yes
Service Deployment	Yes	Yes
Key Material Visibility	Yes	Yes
Reporting	Yes	No
Service Monitoring	Yes	Yes
Device Monitoring	Yes	No
Alerting and Notifications	Yes	No
Licensing	Yes	No
Support Catalog	Yes	No
Software Center	Yes	Yes
Directory Support	Yes	No
Device Log Export	Yes	No
Account Management	Yes	No

Adding and Managing Users

To add or manage the users, click the **Accounts** tab from the menu at the top and then click **Users** from the navigation pane on the left. You'll see the names of all the users on the page that appears, along with details such as **Directory**, **Role**, **Organization**, **Status**, **Name**, and **Username**. Click the **Add User** button and select either **From directory** option to add a new user from a directory or **Locally** option to add a new user by providing the required information.

Add a new user from directory

To add a new user from a directory, you need to:

1. Click the **Add User** button and select the **From directory** option.
2. Search for the user in a specific or all the directories.
3. Select a user by checking the radio button before the user's name and then clicking the **Select User** button.
4. Assign a **Role** and **Organization** for the user.

> **NOTE** Organization can be assigned only if the Role is Application Owner.

5. Enable/disable the **Require two-factor authentication** check box.
6. Add a user by clicking the **Add User** button.

Add a new user locally

To add a new user locally, you need to:

1. Click the Add User button and then select the **Locally** option.
2. Assign a **Role**, **Organization** , and **Password** for the user.
3. Enable/disable the **Require two-factor authentication** check box.
4. Press the **Save** button.

Device Management

This section describes how to perform device management tasks. It contains the following topics:

> "Overview" below
> "Device Management" above
> Managing Device Upgrade from 5.x to 6.x
> "Device Pools" on page 81
> "Troubleshooting Device Connection" on page 83

Overview

You can use CCC to manage, and provision services on Thales Luna Network HSM devices. See the Hardware and Software Requirements section for the minimum device requirements.

There are two levels of device management:

Added devices	When you add a device to CCC, you provide the device address and admin credentials. This information allows CCC to log in to the device as the appliance administrator to perform appliance-level tasks, such as retrieving the device capabilities.
Authorized devices	You must add a device before you can authorize it. When you authorize a device, you provide the HSM SO credentials for the device. This information allows CCC to log into the device as the HSM SO to provision services on the device. **NOTE** You require a remote PED to authorize PED-authenticated devices.

Devices

To add, view, edit, or manage a device, click on the **Devices** tab, and select **Devices** in the navigation frame. All existing devices are listed. You can sort the device list by column, or use the search function to find a specific device:

> Click on the **trash can icon** button in the **Delete** column to delete the device (with confirmation).
> Click on the **Authorize** button in the **Authorization** column to register a currently unregistered device.
> The **Status** column displays an icon for each device. The status indicates whether the device is experiencing any problems.

When you click on a device, its attributes are displayed at the bottom of the page. The information in the device attributes are arranged by tab, as follows:

General	Displays the device name and description. You can edit this information.
Connection	Displays the device address and port. You can update this information as required to re-establish a connection to the device if its software version address, or credentials are changed outside of CCC. CCC connects to devices using the REST API, on port 8443 (default). You must install and configure the REST API on 6.x and 7.0 devices. The REST API is installed with the 7.1 software. It requires configuration.
Device Pool	Displays the device pool that the device belongs to, if any. You can add the device to a device pool, or change its existing device pool. You can add a device to only one device pool.
Authorization	Displays the device's authorization status. You can authorize the device if it is not currently authorized.
Capabilities	Displays the device capabilities. If the device capabilities have changed since the device was added to CCC (for example, after the application of a capability update file (CUF), you can query the device to update the capabilities stored in the device attributes.) **NOTE** 7.x Thales Luna Network HSMs require PPSO partitions. PPSO is enabled by default on Thales Luna Network HSM 7.x devices.
Services	Displays the services provisioned on the device.

Adding Devices

To add a device, you must supply the device address and admin credentials. After you add a device, you can view its capabilities, but you cannot create services on the device until it has been authorized. To authorize a device, you must supply the HSM SO credentials for the device. You can authorize a device when you add it, or you can authorize it at a later time.

> **NOTE** The CCC administrator can add a Luna SA 7.4 FM capability enabled or disabled device to CCC. If the FM capability is enabled, no services can be created on this device but device monitoring is supported.

> **NOTE** The 5.x SAs cannot be added to CCC.

To add a device

1. Click on the **Devices** tab, and select **Devices** in the navigation frame.
2. Click the **Add Device** button. The **Add Device** wizard is displayed.
3. Complete the wizard as follows. You can click **Cancel** at any time to exit the wizard without saving your changes:

General	Enter a name and optional description for the device. This information is used to identify the device in CCC. You can enter any strings you like.
Set Connection	1. Select the device software version. CCC connects to devices using the REST API, on port 8443 (default). You must install and configure the REST API on 6.x and 7.0 devices. The REST API is included in the 7.1 software and requires configuration. 2. Enter the IP address or hostname for the device. If you are not using the default port (8443), enter the port you want to use to connect to the device. 3. Enter the credentials required to log into the device as the Admin user. This information is encrypted and stored in the database to be used by CCC to log into the device. **NOTE** If you add a device using a hostname, CCC does not check to verify that the same device has not already been added using its IP address. As a result, you can add the same device twice – once using its hostname, and once using its IP address. To avoid this issue, we recommend that you always use either hostnames or IP addresses when adding devices.
Verify Connection	Review the device certificate and check the **I have reviewed and trust this host key** or **I have reviewed and trust this certificate** checkbox to accept. If the host key or certificate is not as expected, investigate and correct the problem.
Select Device Pool	Select a device pool for the device, if desired.
Summary	Displays a summary of the information you entered for the device. If the information is not correct, click **Go Back** and update the information as required. Otherwise, click **Finish** to add the device. CCC uses the information you provided to log in to the device. If successful, a success message is displayed and the device is added. You are prompted to authorize the device. Otherwise, an error is displayed, and you can **Go Back** to update the device information as required to resolve the issue. If you want to authorize the device now, click **Authorize now**. You are prompted for the HSM SO password or remote PED address, as relevant. You can authorize the device later by selecting the device and navigating to the **Authorization** tab"Displaying FM Status of a Device" below

Displaying FM Status of a Device

To display whether a device is FM enabled or disabled, click **Devices** in the main navigation. To help find if a device is FM enabled or not, you can select a device displayed in Devices report.

To display FM status

1. Click on the **Devices** tab, and select **Devices** in the navigation frame.
2. Click on a device from the list of devices.
3. Select **Capabilities** tab.

   A new field "**Functional Module (FM)**" with three options is available:

   - Enabled

- Disabled
- Not Supported

> **NOTE** The "**Not Supported**" option is available only for FM incapable devices. It means for the devices prior to Luna SA 7.4, the Functional Module (FM) is not supported.

Managing Device Upgrade from 5.x to 6.x

You may wish to upgrade your managed devices from version 5.x to 6.x or higher to obtain the benefits of 6.x features such as PPSO. If you choose to upgrade your managed devices to 6.x, there is some additional configuration necessary to integrate with CCC 3.7.1.

> **NOTE** We recommend following the best practices for upgrading detailed in the *Thales Luna HSM Documentation*.

To upgrade managed devices from 5.x to 6.x

1. Inform any application users connecting to the devices that their services will be unavailable during the upgrade. You might like to perform the upgrade during a scheduled maintenance window.
2. Upgrade the Thales Luna Network HSM software as detailed in Thales Luna HSM documentation.
3. Set up REST API.
   a. As an appliance user with the Admin or Operator role, obtain and transfer the REST API secure package to the device via SCP/PSCP. Login to the HSM using Security Officer credentials, and install the package. See Thales Luna Network HSM REST API documentation for details.
   b. Set the REST API web service to use a network interface in the HSM. Valid values are all, eth0, eth1, or bond0.

      lunash:>**webserver bind -netdevice** <network_device>
   c. Enable the web service.

      lunash:>**webserver enable**
   d. Generate a REST API service certificate and restart the service. We recommend an RSA certificate type.

      lunash:>**webserver certificate generate -keytype rsa -restart**
4. In CCC, navigate to the **Devices** list and select the recently upgraded device.
5. Click the **Configuration** tab and click **Edit**.
6. In the **Appliance Version** section, select 6.x.

   The **LunaSH Admin Credentials** section changes to **REST API Credentials**, and **Host Key** changes to **Certificate**.
7. Adjust the **Host Address** and **Port Number** as required. Save your changes.
8. Under the **Certificate** section, click **Verify** to view the device certificate.
9. Review the certificate, check the box indicating that you have reviewed and trust the certificate, and then click **Accept**.

10. Update the version of the Thales Luna HSM Client on any crypto application servers that access the devices' services.

    The device is now ready to process incoming cryptographic requests from application users.

Deleting Devices

You can delete a device from CCC only if it is not currently providing any services.

To delete a device

1. Click on the **Devices** tab, and select **Devices** in the navigation frame.
2. After finding the device you want, click on the **trash can icon** in the **Delete** column. A confirmation dialog is displayed.

Device Pools

You can place your devices into device pools, if desired, to help manage your devices. Placing a device into a device pool has no effect on which users or organizations can use the device. You can add a device to one device pool only.

To add, view, edit, or manage a device pool, click on the **Devices** tab, and select **Device Pools** in the navigation frame. All existing device pools are listed. You can sort the list of device pools by column, or use the search function to find a specific device pool. Click on the **trash can icon** button in the **Delete** column to delete the device pool (with confirmation).

When you click on a device pool, its attributes are displayed at the bottom of the page. The information in the device attributes are arranged by tab, as follows:

General	Displays the device name and description. You can edit this information.
Devices	Displays the devices in the device pool.

Adding Device Pools

You can create as many device pools as you like. Device pools can contain an unlimited number of devices.

To add a device pool

1. Click on the **Devices** tab, and select **Device Pools** in the navigation frame.
2. Click the **Add Device Pool** button. The **Create Device Pool** dialog is displayed.
3. Complete the wizard as follows. You can click **Cancel** at any time to exit the wizard without saving your changes:

General	Enter a name and optional description for the device pool. You can enter any strings you like.

Add Devices	You can add devices to the device pool if desired. All devices that are not currently members of a device pool are listed in the **Available Devices** list. You can sort the list of device pools by column, or use the search function to find a specific device pool: > To add a device to the device pool, select a device from the **Available Devices** list and click **Add >>**. > To remove a device from the device pool, select a device from the **Selected Devices** list and click **<< Remove**.
Summary	Displays a summary of the information you entered for the device pool. If the information is not correct, click **Go Back** and update the information as required. Otherwise, click **Create** to create the device pool.

Viewing or Editing Device Pool Attributes

You can sort the device pool list by column heading, or use the search function to find a device pool. When you find the device pool you want, click on the device pool to view or edit its attributes.

To view or edit a device pool's attributes

1. Click on the **Devices** tab, and select **Device Pools** in the navigation frame.
2. After finding the device pool you want, click on the device pool to display the device pool's attributes at the bottom of the page.
3. Use the following tabs to view or edit the device pool attributes:

General	Contains the device pool name and an optional description. > Click **Edit** to edit the information. Click **Save** when done, or **Cancel** to discard the changes and exit edit mode.
Devices	Lists the devices in the device pool: > Click the **Jump to** icon to view detailed information for the device. > Click **Edit** to update the device pool. All devices that are not currently members of a device pool are listed in the **Available Devices** list. The devices in the device pool are listed in the **Selected Devices** list. You can sort the list of device pools by column, or use the search function to find a specific device pool: • To add a device to the device pool, select a device from the **Available Devices** list and click **Add >>**. • To remove a device from the device pool, select a device from the **Selected Devices** list and click **<< Remove**. Click **Save** when done, or **Cancel** to discard the changes and exit edit mode.

Deleting Device Pools

You can delete a device pool at any time. If the device pool contains devices, they are no longer associated with the device pool and become Available Devices.

To delete a device pool

1. Click on the **Devices** tab, and select **Device Pools** in the navigation frame.
2. After finding the device pool you want, click on the **trash can icon** in the **Delete** column. A confirmation dialog is displayed.

Troubleshooting Device Connection

CCC can lose its connection to a device for multiple reasons. The **Device Status** column in the Devices List signifies the severity of the issue.

Device Connection Lost - Device Visible in CCC

If CCC has lost its connection to a device, but the device is still visible within the Devices List there has been some alteration to the HSMs configuration and you must verify the credentials and certificate shared between the device and CCC.

To reconnect a device visible in the CCC Devices List

1. Click on the **Devices** tab, and select **Devices** in the navigation frame.
2. Select the malfunctioning device to display its attributes.
3. Verify the administrator credentials associated with the device are correct.
4. Click **Verify** to confirm that the device certificate matches the certificate stored by CCC
5. If the device is not Authorized, click **Authorize Device**. You will be prompted for the HSM SO password.

Device Connection Lost - Device not Visible in CCC

If the device is no longer visible in the CCC Devices List the device has been deleted. If you would like to use this device you must add the device to CCC. See "Adding Devices" on page 78 for more information.

Absence of a device that was not deleted from CCC may signify corruption in the CCC database. In this event, we recommend following the best practices for ensuring and maintaining database integrity as defined by your Organization's security infrastructure.

General Device Troubleshooting Tips

If you continue to experience problems with the HSM device we recommend connecting to the device using a secure channel, such as the PuTTY SSH client (putty.exe), and verifying the following before attempting to restore the device connection:

- Ensure that the date and time are set correctly
- Ensure that NTLS is bound to the correct Ethernet port
- Ensure that the REST API is installed and configured on the device
- Ensure the webserver on the device is configured and running
- Ensure that the client is registered with the correct ip/hostname
- Ensure that the client is given access to the correct partition
- Check the output of the syslog for any information on errors

Service Management

This section describes how to perform service management tasks. It contains the following topics:

Overview

A cryptographic service is a standalone partition on a Thales Luna Network HSM, or an HA group consisting of multiple partitions, each configured on a different Thales Luna Network HSM, that you manage using CCC. Services are assigned to, and owned by, a specific organization (see "Account Management" on page 75). Only members of the organization that owns the service are able to deploy and use the service for their cryptographic applications.

You can use CCC to import, create, and manage cryptographic services on any devices you manage with CCC. In order to manage services on a device, the device must be authorized to allow CCC to log into the device as the HSM SO (see "Device Management" on page 77).

After you add and authorize a device, you can discover and import any partitions that are already provisioned on the device, or create new services on the device. Once you import or create a service, you can manage it with CCC.

The service management functions are grouped under the **Crypto Services** tab. Under **Services** you can sort the services list by column, or use the search function to find a specific service:

> Click on the **trash can icon** button in the **Remove** column to either detach or delete a device or organization from the services menu.

> The **Status** column displays an icon for each service. The status indicates whether the service is experiencing any problems.

The service status is displayed in the status column. If you hover over the icon with your cursor a relevant tooltip will display.

Discovering and Importing Existing Unmanaged Services

You can use the **Import Partitions** function to discover any partitions provisioned on your managed devices that do not already exist as services in CCC. The Import Partitions function queries each managed device, in turn, to find any partitions that are not currently in the CCC database. CCC examines the partitions on each device to determine if they represent standalone services or HA Group services. The results are displayed in a table that includes information for each partition, such as size, number of objects, and registered clients.

> **NOTE** If you import an existing partition that uses both the Per-Partition Security Officer (PPSO) and Secure Trusted Channel (STC) features, CCC can only view partition details and delete the partition. CCC cannot modify the partition or give access to Application Owners. This is because the Partition SO can only access and modify the partition through the existing STC client that was established before import.

Partitions that appear to be part of an HA group (that is, those that are the same size, contain the same number of objects, and have the exact same set of clients) are grouped together and assigned the same default HA Group label (HA<n>, for example, HA3). Partitions which use STC and do not have the Per-Partition Security Officer (PPSO) feature enabled are grouped based on the STC fingerprint. If two or more partitions on the same appliance meet the criteria for belonging to the same HA group, only one is selected, as follows:

- if one of the partitions has the same name as the other partitions in the HA group, it is selected.
- if none of the partitions have the same name as the other partitions in the HA group, the first matching partition is selected.

> **NOTE** The default HA Group label assigned to any discovered HA groups is temporary only, and is not the label assigned to the HA group when it was created. After confirming the grouping, you must change the default label to the actual label, as determined using VTL, to ensure that CCC can successfully manage the service.

The user is allowed to perform Import Partitions for an HA group only if the selected partitions belonging to an HA group should meet the following conditions:

- Partitions should be of same size.

> **NOTE** If the selected partitions are of different sizes, the following error message displays: "Cannot import an HA group that contains partitions with different sizes".

- Two or more partitions should have same authentication mechanism such as PED or Password type.

> **NOTE** If two or more selected partitions have different authentication mechanisms such as PED or Password type, the following error message displays:
> "Cannot import an HA group that contains partitions from a mix of Password and PED type devices".

- Two or more partitions should belong to different devices.

> **NOTE** If two or more selected partitions belong to same device, the following error message displays:
> "Cannot import an HA group that contains two or more partitions from the same device".

- Two or more partitions should have same transport (NTLS or STC) types .

> **NOTE** If two or more selected partitions have a mix of different transport (NTLS/STC) types, the following error message displays:
> "Cannot import an HA group that contains partitions with a mix of different transport (NTLS/STC) types.

After examining and verifying the data in the table, you must edit the table to specify a name, organization, and optional description. After providing the required information, you can import the partitions as services.

See "Discovering and Importing Unmanaged Partitions" on the next page for detailed procedures that describe how to import partitions and add them as services to CCC.

Creating New Services

To create a service:

- choose a template that defines the characteristics of the service you would like to create. New services are defined using templates, which specify the type, size, and capabilities of a service. See "Creating and Managing Service Templates" on page 89 for detailed procedures that describe how to create, edit, and manage service templates.
- specify the device(s) you want to use to host the service.
- specify the organization whose users are able to deploy the service.
- optionally initialize the service with an option to activate, if the service is a PED-authenticated Per-Partition Security Officer (PPSO) service. See "Initializing a Service" on page 93 and "Activating a PED-Authenticated Service" on page 95.

When you create a non-PPSO service, the resources required to provide the service are reserved in CCC, but the actual partition(s) are not created on the device(s) until the service is initialized. When you create a PPSO service on CCC, an uninitialized partition is also created on the specified device(s). Services can be initialized by the CCC Administrator, or by an Application Owner that is a member of the organization that owns the service.

In addition, you can create a service and indicate in the service template that the new service should use Secure Trusted Channel (STC) links for client connections. The STC status is "Pending" until an Application Owner deploys the service, which enables the STC policy on the partition(s) and establishes the STC link to the Application Owner's Thales Luna HSM client.

See "Creating New Services" on page 92 for detailed procedures that describe how to create a new service.

Managing your services

After you have added or created a service, you can view or edit its attributes to do the following:

- change the service name, description, or organization
- initialize the crypto user role on a PPSO service
- activate a role on a PPSO PED-based service
- remove the service from CCC
- add a partition
- remove a partition
- delete the service it if it is no longer required

> view the service status

See "Managing Services" on page 95 for detailed procedures that describe how to view, edit, remove, or delete services.

Discovering and Importing Unmanaged Partitions

Devices you add to CCC may already contain partitions and HA groups. Alternatively, although it is not recommended, an Administrator may have created partitions or HA groups on a managed device using the command line tools after you added the devices to CCC. You can use the **Import Partitions** function to discover any unmanaged partitions, with the option of importing them into CCC as services. You can use the **Import Partitions** function at any time to discover unmanaged partitions on your managed devices. To ensure that all HA groups are discovered, all authorized devices are included in the search.

If you attempt to import a number of partitions exceeding the partitions available, the **Import Partitions** option is disabled. CCC requires that you reduce the number of partitions for import to a value equal to, or less than, the number of available partitions, then re-attempt import.

The Import Partitions function consists of three distinct phases:

1. **Discovery**

   In this phase, CCC logs in to each authorized device to find any partitions that are not in the CCC database.

2. **Verification and data entry**

   The discovered partitions are returned in a table, sorted by service type (standalone partitions or partition HA groups), which you must then edit to provide the information required to create services for the discovered partitions (service name, organization, and optional description). You can choose to import all of the discovered partitions, or you can delete any partitions from the table that you do not want to import at this time. To add a partition or HA group as a service in CCC, you must enter a service name and choose the organization that will own the service. You can also enter an optional description for the service.

   > **NOTE** Any partitions that you delete from the table are removed from the current import only. You can import them later by running the **Import Partitions** function again.

   Edits to the table are saved automatically and persist between login sessions. If you select **Crypto Services** > **Import Partitions** while you have a currently saved table, the discovery portion of the Import Partitions function is skipped, and the saved table is displayed. The Import Partitions page shows when the table was first created and last edited.

   > **NOTE** Your data may not be preserved, depending on your browser settings. If you have configured your browser to discard history on exit, all data will be lost.

3. **Service creation**

   Once you have verified the data in the table, supplied a service name and optional description, and chosen the organization that will own the service, click **Finish Import** to create services for the partitions and HA groups. Once complete, you are redirected to the Crypto Services page, where you can manage the partitions and partition HA groups in CCC.

> **NOTE** Importing partitions that have both the STC and PPSO policies into CCC allows you to view partition information, but functionality is reduced as CCC is not established as a secure endpoint for the existing STC connection. You can detach or delete the service, or change the service name, description, or organization.

To discover and import unmanaged partitions

1. Click on the **Crypto Services** tab, and select **Import Partitions** in the navigation frame:
   - if you do not have a currently saved partition import table, the Import Partitions splash page is displayed. Go to the next step.
   - otherwise, the currently saved partition import table is displayed. Go to step 3.
2. Click on the **Get Started** button to begin the discovery process. The Finding Partitions progress dialog is displayed.

   The discovery process may take some time to complete, depending on the number of devices that must be queried. When the discovery is complete, a table listing all of the discovered partitions is displayed. A tutorial overlay is provided that explains how to use the table to verify the discovered partitions, and import them into CCC as services.
3. Although CCC attempts to identify the partitions by service type (standalone partition or partition HA group), it is strongly recommended that you examine the data in the table and verify its accuracy, especially for any HA groups that have been identified. For example, you may want to log in to each client that uses an HA group to verify that the HA group members match those listed in the table.
4. If you need to make any changes, you can do so as follows:
   - to move a partition to a different HA group, type the correct HA group name for the partition in the HA Group field.
   - to remove a partition from an HA group and make it a standalone service, delete the suggested HA group name from the HA Group field.
   - to add a partition identified as a standalone service to an HA group, type the name of the HA group you want to add it to in the HA Group field.
5. For each HA group you want to import, log in to one of the clients that use the HA group and use the **vtl haAdmin show** command to determine the actual HA Group Label for the HA group. Delete the default HA Group label (HA_<n>), and replace it with the actual HA Group Label.
6. After you have verified the HA groupings and deleted any partitions from the table that you do not want to import at this time, edit the table to provide the following information for each partition or HA group. The values for service name, description, and organization are automatically replicated to each partition in an HA group as you enter them:

HA Group	Enter the HA Group Label string for the HA group as determined using the **vtl haAdmin show** command.
Service Name	Enter the name that will be used to identify the service in CCC. This is limited to 28 characters.
Description	Enter a description for the service. This field is optional.

Organization	Choose the organization that will own the service. If the organization does not exist, you must create it. See "Account Management" on page 75.

7. After you provide a service name, optional description, and organization for each partition or HA group, click **Finish Imports** to create a service for each partition or HA group.

   The Services page is displayed, listing the newly added services. You can now manage the services as described in "Managing Services" on page 95.

Canceling an Import

If you want to restart the import process click **Cancel**. The current table is deleted. Click on **Crypto Services** > **Import Partition** to restart the discovery process and create a new table.

Creating and Managing Service Templates

When you create a service, you must specify a template for the service. Service templates specify the type, size, and capabilities of services created using the template. Service templates are reusable, allowing you to create templates for specific application types that can be used to quickly and easily create services for specific applications.

To add, copy, view, edit, or manage a service template, click on the **Crypto Services** tab, and select **Service Templates** in the navigation frame. All existing service templates are listed. You can sort the list of service templates by column, or use the search function to find a specific service template. Click on the **Copy Template** icon to copy and edit a service template. Click on the **trash can icon** in the **Delete** column to delete a service template (with confirmation).

When you click on a service template, its attributes are displayed at the bottom of the page. The attributes are arranged by tab, as follows:

General	Displays the template name and description. You can edit this information.
Capabilities	Displays the type, size, and capabilities of services created using the template. You can edit this information.

Creating Service Templates

You can create as many service templates as you like to define the different types of services you need to create.

To add a service template

1. Click on the **Crypto Services** tab, and select **Service Templates** in the navigation frame.
2. Click the **Add Service Template** button. The **Create Service Template** dialog is displayed.
3. Complete the wizard as follows. You can click **Cancel** at any time to exit the wizard without saving your changes:

General	Enter a name and optional description for the service template. You can enter any strings you like.

Set Capabilities	Specify the type, size, and capabilities of services to be created using this template, as follows: > **Service type**: Choose **HSM Partition** to create a standalone service on a single device. Select **HSM Partition HA Group** to create an HA group using two or more devices. > **Partition size (bytes)**: Specify the size of the partition(s), in bytes, used to provide services created using this template. > **Per-Partition SO**: Click this checkbox if you want the services created using this template to have their own security officer (SO). Per-Partition SO is supported on devices with firmware 6.22 or higher, and with the Per-Partition SO capability upgrade (CUF) installed. **NOTE** Per-partition SO is the mandatory setting for 7.x devices, and is enabled by default. > **Secure Trusted Channel**: Click this checkbox if you want the services created using this template to connect to Application Owner clients using Secure Trusted Channel (STC) instead of the default NTLS connection. Secure Trusted Channel is supported on devices with software 6.2.1 or higher, firmware 6.24.2 or higher, and the STC HSM policy enabled. When you create a service with the capability in the template, the STC status is "pending" until an Application Owner deploys the service, which enables the STC partition policy, and establishes the STC link. > **Device Capabilities**: Choose the following options to specify the capabilities of the device (s) used to host services created using this template. • **Performance**: Select **Low** or **High** performance. • **Authentication**: Select **PED** or **Password**. • **Backup**: Select **Cloning** or **Key Export**.
Summary	Displays a summary of the information you entered for the service template. If the information is not correct, click **Go Back** and update the information as required. Otherwise, click **Finish** to create the service template.

Copying and Editing an Existing Service Template

You can copy an existing template and edit it as required to create a new service template.

To copy and edit an existing service template

1. Click on the **Crypto Services** tab, and select **Service Templates** in the navigation frame.
2. Find the service template you want to copy. To help find a service template, you can sort the service list by column heading, or use the search function.
3. Click on the **Copy Template** icon. The **Create Service Template** wizard is displayed, with the fields pre-filled with the values from the copied service template.
4. Complete the wizard, as described in "Creating Service Templates" on the previous page.

Viewing or Editing the Service Template Attributes

You can sort the service template list by column heading, or use the search function to find a service template. When you find the service template you want, click on the service template to view or edit its attributes.

To view or edit a service template's attributes

1. Click on the **Crypto Services** tab, and select **Service Templates** in the navigation frame.
2. After finding the service template you want, click on the service template to display the service template's attributes at the bottom of the page.
3. Use the following tabs to view or edit the service template attributes:

General	Contains the service template name and an optional description. > Click **Edit** to edit the information. Click **Save** when done, or **Cancel** to discard the changes and exit edit mode.
Capabilities	Displays the type, size, and capabilities of services created using the template. Click **Edit** to edit the service template, as follows > **Service type**: Choose HSM Partition to create a standalone service on a single device. Select HSM Partition HA Group to create an HA group using two or more devices. > **Partition size**: Specify the size of the partition(s) used to provide services created using this template. > **Per-Partition SO**: Click this checkbox if you want the services created using this template to have their own security officer (SO). Per-Partition SO is supported on devices with firmware 6.22 or higher, and with the Per-Partition SO capability upgrade (CUF) installed. **NOTE** Per-partition SO is the mandatory setting for 7.x devices, and is enabled by default. > **Secure Trusted Channel**: Click this checkbox if you want the services created using this template to connect to CCC using Secure Trusted Channel (STC) instead of the default NTLS connection. Secure Trusted Channel is supported on devices with software 6.2.1 or higher, firmware 6.24.2 or higher, and the STC HSM policy enabled. The STC link is established in ccc_client when the service is deployed by an Application Owner. > **Device Capabilities**: Choose the following options to specify the capabilities of the device (s) used to host services created using this template. • **Performance**: Select Low or High performance. • **Authentication**: Select PED or Password. • **Backup**: Select Cloning or Key Export. Click **Save** when done, or **Cancel** to discard the changes and exit edit mode.

Deleting Service Templates

You can delete a service template at any time.

To delete a service template

1. Click on the **Crypto Services** tab, and select **Service Templates** in the navigation frame.
2. After finding the device pool you want, click on the **trash can icon** in the **Delete** column. A confirmation dialog is displayed.

Creating New Services

To create a service, you must specify the service template for the service, the device(s) used to host the service, and the owner organization. After you add a service, you can view its capabilities and host device, but an Application Owner cannot deploy a service until it has been initialized. You can initialize a service when you create it, or you can leave it uninitialized. Uninitialized services can be initialized by the CCC Administrator, or by an Application Owner that is a member of the organization that owns the service.

To create a service

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame.
2. Click the **Create Service** button. The **Create Service** wizard is displayed.
3. Complete the wizard as follows. You can click **Cancel** at any time to exit the wizard without saving your changes:

General	Enter a name and optional description for the service. This information is used to identify the service in CCC. You can enter any strings you like. After you add the service, you can change its name or description by editing the service attributes. See "Service Management" on page 84.
Choose Template	Choose a template from the list that defines the type of service you want to create. To help find a service template, you can sort the list by column heading, or use the search function. **NOTE** You can view service template details by hovering over the information (i) icon associated with the service template.
Add Devices	Select the device, or devices, used to provide the service. If the service is an HSM partition HA group, you must specify each device (minimum of 2) that will be used to provide the HSM partition HA group. To select a device, click on the device in the **Available Devices** window and click **Add** to move it to the **Selected Devices** window. You can use the search function to help find a device, if necessary. To deselect a device, click on the device in the **Selected Devices** window and click **Remove** to move it to the **Available Devices** window.
Assign Organization	Choose the organization that will own the service from the list. To help find an organization, you can sort the organization list by column heading, or use the search function. After you add the service, you can change the organization that owns the service by editing the service attributes. See "Service Management" on page 84.
Summary	Displays a summary of the information you entered for the service. If the information is not correct, click **Go Back** and update the information as required. Otherwise, click **Finish** to create the service. If successful, a success message is displayed and the service is added. You are prompted to initialize the service. See "Initializing a Service" on the next page Otherwise, an error is displayed, and you can click **Go Back** to update the device information, as required, to resolve the issue.

Initializing a Service

You must initialize a service before you can use it. To initialize a service, you must specify or create the following:

> the initial credentials for the roles that will own or use the service:
  - for services without PPSO enabled, you initialize the credentials for the partition owner (crypto officer) role.
  - for services with PPSO enabled, you initialize the credentials for the partition SO and crypto officer roles. You also have the option to initialize the crypto user role.

> the cloning domain for the service. You can only clone objects between HSMs that are in the same cloning domain. Cloning is used to perform operations such as backup/restore.

You can initialize a service when you create it, or you can leave it uninitialized until it is ready to be deployed. Uninitialized services can be initialized by the CCC Administrator, or by an Application Owner that is a member of the organization that owns the service.

Initializing a PED-authenticated Service

To initialize a PED-authenticated service, you need a remote PED and the orange PED key(s) encoded with the Remote PED Vector (RPV) for the Thales Luna Network HSM appliance(s) that provides the service. You also need to imprint or provide the role and domain PED keys for the service. as follows:

> for non-PPSO services, you initialize the credentials for the partition owner (crypto officer) and set the cloning domain for the service, by providing or imprinting the crypto officer (black) and domain (red) PED keys.

> for PPSO services, you initialize the credentials for the partition SO, crypto officer, and (optionally) crypto user roles, and set the cloning domain for the service, by providing or imprinting the partition SO (blue), crypto officer/crypto user (black/gray), and domain (red) PED keys.

Contact the CCC Administrator to get any keys you may require.

To use a remote PED with CCC, you need to install the Thales Luna HSM client, including the Remote PED Server option, on the computer you will use to access CCC, or on a separate computer you will use for the remote PED. After installing the Thales Luna HSM client, use LunaCM to configure the Remote PED Server so that you can connect to it from CCC. Refer to the Thales Luna HSM documentation for more information.

To initialize a PED-authenticated service

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all currently provisioned services. Any uninitialized services have an **Initialize** button in the Initialization State column. To help find a service, you can sort the service list by column heading, or use the search function.
2. Click on the **Initialize Service** link for the service you want to initialize. The **Initialize Service** wizard is displayed. Complete the wizard as follows:

Define Partition	Enter a label for the partition used to provide the service.

Initialize Roles	Enter the IP address of your remote PED server. The default port is auto-filled. If you are not using the default port, enter the Remote PED server port. For PPSO services, enter the challenge password for the crypto officer and (optionally) crypto user roles. The challenge password is the password used to authenticate to the role after it is activated. Click **Next** and respond to the prompts on-screen and on the PED. For non-PPSO services, the PED generates and displays a 16-digit challenge password. Record this challenge password. It is necessary for service activation.
Activate Roles	To activate the roles you initialized, click the **Activate Crypto Officer** and (optionally) **Activate Crypto User** checkboxes. You cannot activate the crypto user without also activating the crypto officer. You can activate the roles later for PPSO services, if desired, by editing the service attributes. For services which have the both the PPSO and the STC feature enabled in the template, you can activate the roles any time until an application user deploys the service, which establishes the STC link and precludes further changes through CCC. Click **Finish** to initialize the service. Observe the progress messages to verify success.

Initializing a Password-authenticated Service

To initialize a password-authenticated service, you need to enter passwords for the roles you wish to initialize, and specify the cloning domain for the service, as follows:

> for non-PPSO services, you enter an initial password for the crypto officer and set the cloning domain for the service.

> for PPSO services, you enter an initial password for the partition SO, crypto officer, and (optionally) crypto user roles, and set the cloning domain for the service.

To initialize a password-authenticated service

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all currently provisioned services. Any uninitialized services have an **Initialize Service** button in the Initialization State column. To help find a service, you can sort the service list by column heading, or use the search function.
2. Click the **Initialize Service** link for the service you want to initialize. The **Initialize Service** wizard is displayed. Complete the wizard as follows:

Define Partition	Enter a label and cloning domain for the partition used to provide the service.
Initialize Roles	Set the initial password for the Crypto Officer. For PPSO services, you also set the initial password for the Security Officer, and optionally for the Crypto User. Click **Finish** to initialize the service. Observe the progress messages to verify success. **NOTE** For a service which used STC and PPSO, after the service is deployed you cannot initialize the Crypto User role through CCC.

Activating a PED-Authenticated Service

You can activate a role on a PED-authenticated service to allow the role to authenticate to the service using a challenge password only, without PED interaction. You can activate a service when you initialize it, or later, by selecting the service and navigating to the **Partitions** tab. See "Service Management" on page 84

Limitations

- You can activate PPSO services only. Use LunaCM to activate a non-PPSO service.
- Services that have both PPSO and STC enabled cannot be activated after the service is deployed to an Application Owner. This is because after the STC link is established, the Partition SO can only access and modify the partition through the STC link with the Thales Luna HSM client, not through CCC.

Managing Services

After you have added or created a service, you can view or edit its attributes, remove it from CCC, or delete it if it is no longer required.

To manage your services, click on the **Crypto Services** tab, and select **Services** in the navigation frame. All existing services are listed. You can sort the service list by column, or use the search function to find a specific service:

- Click on the **dropdown** button in the **Remove** column to detach or delete the service (with confirmation).
- Click on the **Initialize** button in the **Initialization State** column to initialize a currently uninitialized service. See "Initializing a Service" on page 93.
- There is a **Status** column displaying an icon for each service. The status indicates whether the service is running properly or offline.

When you click on a service, its attributes are displayed at the bottom of the page, arranged by tabs.

Viewing or Editing Service Attributes

Click on a service to display its attributes the bottom of the page. To help find a service, you can sort the service list by column heading, or use the search function.

To view or edit service attributes

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all added services.
2. After finding the service you want, click on the service to display its attributes.
3. Click on a tab to view, edit, or refresh the service attributes, as follows:

General	Displays the service name and description, the organization that owns the service, who created the service, and when it was created. You can edit the service name, description, organization, or HA group label.

Capabilities	Displays the service type, partition size, authentication type, and capabilities of the host device. **NOTE** The CCC administrator can view and edit the partition size in a service. For more details, refer to "Modifying partition size " on the next page to know the steps to configure the partition's size as per the required usage.
Partitions	Displays the name of the host device(s). If the service is initialized, the name(s), label(s), serial number(s), appliance version(s), and device firmware version(s) of the partition(s), and that provide the service are also displayed. The Admin user can add and initialize partitions to any single or HA service. One or more partitions can be removed from an HA service. For PPSO services, additional functions are available: Click on **Initialize Crypto User** to set the initial credentials for the crypto user role. Click on **Activate Roles** to activate a role so that it can use a challenge password to connect to a PED-authenticated service without PED interaction. You are prompted to enter the challenge password(s) for the role(s). This function applies to PED-based services only.
Keys	Displays the Label, Type, Handle, Fingerprint, Algorithm, and Bit Size of the keys present on partitions associated with a service. To view the key attributes, you must authenticate as the Crypto Officer by providing a Crypto Officer Password. For PED services, you must provide valid Remote PED Server IP Address and Port. **NOTE** In case of a PED service, if the CO role is activated, you are not required to provide Remote PED Server IP address and port details. CCC establishes an NTLS session with the partitions to fetch the partition object information. You can use the Log Off Session button to terminate the NTLS session. A session that remains idle for 3 hours gets automatically terminated. **NOTE** To ensure that this feature works properly, it's recommended that you use Lunaclient 7.1 or above on the CCC server. **NOTE** It is recommended that you should not use the CCC server to create an NTLS connection via LunaCM or LunaSH as that can lead to errors while displaying key attributes. Instead, you can use the CCC Client to create an NTLS connection. **NOTE** For non-PPSO PED HA services, activate the crypto officer manually. Before running key export, refer to "Activating a non-PPSO PED-Authenticated HA Group" on page 151. **NOTE** As part of the key attributes retrieval on HA service, CCC will sync objects created across all member partitions of that HA group. **NOTE** If you are unable to retrieve the keys for 6.x Non-PPSO partitions, refer to "Administration Issues" on page 159 for a resolution.

Clients	Displays the status, host address, fingerprint, and last registration of the Thales Luna HSM client workstation(s) that the service is deployed on, if it is currently deployed. **NOTE** When an added partition is initialized or an initialized partition is removed from a service, status of clients already associated with the service changes to error status icon indicating that these clients must be re-registered to sync to the changes of the service.

Modifying partition size

After creating a service, CCC administrator can view and edit the size of partitions in a service to configure the partition's size as per their required usage.

The restriction on the partition size is defined as below:

> The minimum partition size can be 1000 bytes.

> The maximum partition size can be 99999999 bytes.

To modify partition size

1. Click **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all added services.
2. Click a service. A list of attributes in the form of tabs displays.
3. Click **Capabilities**.
4. Click **Edit** button displayed under Capabilities tab.
5. Enter a new numeric value in the **Partition size (bytes)** text box.

> **NOTE**
> 1. CCC administrator is not allowed to enter the alphanumeric value in the **Partition size (bytes)** text box.
>
> 2. If CCC administrator enters an value to configure the partition size which is not allowed as per available device memory size, a modal window with an error message displays.

6. Click on **Save**. If the updated partition size is saved successfully, a modal window displays with a success message.
7. Click **Close** to close the modal window.

> **NOTE**
> 1. In case CCC stops functioning due to a network issue, then the updates are rolled back and an error message displays to notify the CCC administrator to try again later.
>
> 2. If one or more devices are offline while saving the updated partition size, an error message displays to notify the CCC administrator to try again when all the devices are online.
>
> 3. If no space is available on devices while modifying the partition size, an error message displays.

Adding a Partition to a Service

As a CCC administrator, you can add a partition to either bring failover support by converting single partition service to HA, or to increase the redundancy by adding more members to the HA group.

To add a partition to a service

1. Click **Crypto Services** tab, and selected Services in the navigation frame to display a list of all added services.
2. Click a service. A list of attributes in the form of tabs displays.
3. Click **Partitions**.
4. Click **Add Partition**s. The Add Partitions modal window displays.
5. Click **Add** to add the devices displayed under **Available Devices** or click **Close** to close the Add Partitions modal window.

> **NOTE** The devices which are already associated with service will not display under Available Devices list.

6. Click **Next**. The confirmation modal window displays.
7. Click **Add Partitions** to add the partitions to the service.

   Once the CCC administrator clicks **Add Partitions**, a modal window with success message displays.
8. Click **Initialize now** to initialize the added partitions or **No, close** to close the modal window.

> **NOTE**
> 1. The new uninitialized partitions added are displayed in a separate grid with header "**Uninitialized Partitions**" below the initialized partitions with "**Initialize Partitions**" option on right side.

Initializing an added partition

You must initialize an added partition before you begin to use this partition. You can initialize an added partition as a CCC administrator or an application owner.

To initialize an added partition

1. Click **Initialize now** link displayed on success modal window while adding a new partition.

2. The **Initialize New Partitions** modal window with a caution displays with following three tabs:
   - Important
   - Define Partition
   - Initialize Role

   > **NOTE** The **Important** tab displays a caution to initialize new partitions with same cloning domain and role credentials to prevent zeroizing of the existing partitions.

3. Click **Next**. The **Define Partition** tab displays with disabled Partition Label.
4. Enter the Cloning Domain and confirm it.
5. Click **Next**. The Initialize Roles tab displays.
6. Enter the **Crypto Officer Password** and confirm it.

7. Select **Initialize Crypto User** checkbox to initialize Crypto User credentials.

Applicable in case of PPSO Password and PED Services:

	New Partition	Old Partition	Behavior	
Initialize CU	Yes	Already initialized	No change on old partition	New: Initialized Old: Initialized
Initialize CU	Yes	Not initialized	Old partition will also be initialized	New: Initialized Old: Initialized
Initialize CU	No	Already initialized	No change on old partition	New: Uninitialized Old: Initialized
Initialize CU	No	Not initialized	No change on old partition	New: Uninitialized Old: Uninitialized

Applicable only in case of PPSO PED Services:

	New Partition	Old Partition	Behavior	
Activate CU	Yes	Already activated	No change on old partition	New: Activated Old: Activated
Activate CU	Yes	Not activated	Old partition will also be activated	New: Activated Old: Activated
Activate CU	No	Already activated	No change on old partition	New: Not activated Old: Activated
Activate CU	No	Not activated	No change on old partition	New: Not activated Old: Not activated

8. Click **Initialize New Partitions**. The Partitions successfully initialized modal displays.
9. Click **Close** to close the modal.

> **NOTE**
> 1. When an added partition is initialized or an initialized partition is removed from a service, status of clients associated with the service changes to error status icon indicating that these clients must be re-registered to sync to the changes of the service.
>
> 2. When a partition is added and initialized, the CCC user should refers "To deploy a service" on page 146 to repair the clients for authorizing the added partitions.

> **NOTE** The CCC Administrator can also initialize a partition by clicking **"Initialize Partitions"** option under Firmware column of Uninitialized Partitions section and follow steps **2-9** to initialize an added partition.

To Initialize New Partitions from the list of all provisioned services

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all currently provisioned services.

> **NOTE** Any provisioned services that have some of the new partitions in uninitialized state have an **Initialize New Partitions** link in the Initialization State column.

2. Click **Initialize New Partitions** link in the Initialization State column.

> **NOTE** The CCC Administrator can follow steps **2-9** of "To initialize an added partition" on page 98 to initialize an added partition.

Removing a Partition from HA Group

As a CCC administrator, you can remove a partition from an HA group to save the memory on the device or to re-use the partitions.

> **NOTE** It is important for CCC administrator to clone any required key material before deleting the partition.

To remove a partition from HA group

1. Click **Crypto Services** tab, and select **Services** in the navigation frame to display a list of all added services.
2. Click a service. A list of attributes in the form of tabs displays.
3. Click **Partitions**.
4. Click the **dropdown icon** displayed in rightmost column and select **Remove Partition**. A confirmation dialog displays.
5. Click **Yes remove partition** in the dialog to remove the partition from an HA group or click **No, cancel** to close the dialog.

> **CAUTION!** Once a partition is removed, the action cannot be undone.

> **NOTE** Partition deletion functionality is applicable only on HA services. If the user tries to remove the last partition from a HA group, an error message displays.

> **NOTE** The CCC administrator cannot perform partition removal operation on a single HSM service.

Detaching or Deleting Services

You can detach or delete a service if you no longer wish to manage it using CCC, or you can delete a service if it is no longer required:

- Detaching a service only removes it from CCC. It does not affect the associated partition(s) used to provide the service, or the objects they contain.
- Deleting a service removes it from CCC and deletes the partition(s) used to provide the service and any objects they contain. Services are normally deleted by the Application Owner.

To detach a service

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame.
2. After finding the service you want, click on the **dropdown icon** in the **Remove** column and select **Detach service**. A confirmation dialog is displayed.

To delete a service

> ****WARNING** Deleting a service deletes the partition(s) used to provide the service and all objects in the partition(s).**

1. Click on the **Crypto Services** tab, and select **Services** in the navigation frame.
2. After finding the service you want, click on the **dropdown icon** in the **Remove** column and select **Delete service**. A confirmation dialog is displayed.

Service Monitoring

The Service Monitoring feature is introduced in the left navigation under Monitoring & Reports tab. It helps the CCC Administrator and the CCC Application Owner to view the list of initialized and partially initialized services with average operations count per second in a tabular format. It has four important sections:

- Viewing Service Monitoring Table
- Displaying Partition Cards
- Viewing Aggregated Current Count of Operations for Service
- Viewing Operations Per Second over Time
- Viewing Average Operations Per Second over Time
- Viewing Client Connection Information
- Viewing Custom Notifications

> **NOTE** The "**Custom Notifications**" section available under Service Monitoring feature is accessible only by the CCC administrator.

> **NOTE** The CCC Service Monitoring feature will require a license that includes monitoring. If the monitoring license is not available, a "**Monitoring license required**" message displays prompting CCC administrator to upgrade the application license. For application owner, the message displays prompting the CCC app owner to contact the CCC administrator to upgrade the application license.

> **NOTE** The CCC Administrator must enable the HSM policy 49 manually via LUSH command on device version 7.3.0 or later.

Viewing Service Monitoring Table

1. Click the **Monitoring & Reports** tab, and select **Service Monitoring** in the left navigation frame.

The columns in the table provides the following details:

Status	An indication of service status. **Checkmark icon** (): All the associated devices are up and running. **Caution icon** (): One or more of the associated devices are down. **Error icon** (): All the associated devices are down.
Service Name	Specifies the name of the service.
Organization	Specifies the name of the organization.
Partition Count	Specifies the number of partitions in a service.
Average Operations/Sec	Specifies the sum of all operations from all partitions in a service divided by number of seconds data was collected (up to 90 days max). **NOTE** If all the devices are offline for a particular service, then --- ops/sec is displayed.

Displaying Partition Cards

1. Click a service from the table list.
2. The partition card displays the following information related to an added partition in the service:
   a. The name of the partition.
   b. The status of the partition as follows:
      i. Online (with a green check mark icon).
      ii. Offline (with a red error icon).

> **NOTE** If the partition is Online and uninitialized, a message displays with a blue exclamation icon to indicate the status: "Online - Partition Not Initialized".

      iii. The name of the device with which the partition is associated.
      iv. The Last counter reset value.
      v. A toggle switch to include the partition metrics in the aggregated service data card.

> **NOTE** If the partition has no data, the toggle switch is disabled and a message displays with a yellow exclamation icon to indicate the status: "No Data Available".

Viewing Aggregated Current Count of Operations for Service

To view aggregated current count of operations for Service:

1. Click a service from the table list.
2. The aggregate monitoring information for all selected partitions in the service displays in a doughnut chart.
3. Click the toggle switch on the partition card to select or deselect the partition card to view selected or full count of operations.

> **NOTE** The administrator can use the toggle switch to modify the monitoring information displayed in the doughnut chart.

Viewing Operations Per Second over Time

1. Click a service from the table list. A line graph showing aggregate operations per second over the time displays.
   - The **x** axis of the graph represents time.
   - The **y** axis of the graph represents operations per second. The value of the operations per second is dynamic based on the data.

   > **NOTE** By default, all the partitions in the service are selected to display the aggregate value of operations per second over the time associated with the service as a line graph.

   > **NOTE** The mathematical formula to display the aggregate operations per second on Line chart is: **ops/sec = (Sum of no. of operations between two data points)/(Number of seconds in that interval)**.

2. Click the toggle switch on the partition card to select or deselect the partition card.

   > **NOTE** If no partitions are selected, an empty state for line graph displays with a message: " "**Please ensure at least 1 partition is toggled on to view data**".

   > **NOTE** If there is not enough data to populate the line graph, a message indicating no available data displays prompting the user to select a different time period.

   The CCC administrator can filter the statistics of line graph by using two drop down filter options:

   c. **Operations Type**

   d. **Time frame**

   When the CCC administrator selects an option from either of the two drop down filters, the data displayed in the line graph updates according to the selected option.

Viewing Average Operations Per Second over Time

1. Click the **Show Average Operations/Sec trend line** check box. A second blue line appears displaying the average operations per second over the time.

> **NOTE** By default, the **Show Average Operations/Sec trend line** check box is unchecked.

- The **x** axis of the graph represents time.
- The **y** axis of the graph represents average operations per second.

The value of the average operations per second is dynamic based on the data.

> **NOTE** The mathematical formula to display the average operations per second on Line chart is: **Avg ops/sec =** (**Sum of ops/sec)/(Number of ops/sec data points**) collected over a time period.

Viewing Client Connection Information

1. Click a service from the table list. The **Client Connections** tab displays under **Service Data** section.
2. Click **Client Connections** tab under Service Data section.

   The network information of all the clients connected with partitions of selected service displays. NTLS client connections display in the table:

The columns in the table provides the following information:

Device Address	Specifies the IP address of device on which partition is hosted.
Client Address	Specifies the IP address of Client machine.
State	Specifies the state of the client connection. There are two types of states: > **Established**: It indicates the client connection is established. > **Closed** : It indicates the client connection is closed.
Protocol	Specifies the network protocol with which client is communicating with the device.
Connected Partition	Specifies the partition of the service which is connected with particular client.

Viewing Custom Notifications

To enable custom notifications for the selected service, activate the toggle switch.

> **NOTE** By default, this service uses the global notification event settings. The CCC administrator can enable the custom notification toggle switch to overwrite global settings for this service only.

The service level settings consists of a "**Moving average time period**" drop down with multiple options of time periods that allows the CCC user to choose a time period for sending service alerts on crypto rate fluctuations.

> **NOTE** The different options available for "Moving average time period" are **30 Minutes,1 hour, 4 hours, 8 hours, 1 day, 3 days, 7 days, 30 days, and 90 days.**

> **NOTE** A minimum of 30 minutes data is required for a Moving average time period option to send a crypto operation fluctuation alert. For example, if the application starts capturing data at 11:00 AM, it sends an alert at 11:30 AM onwards. However, if the application starts at 11:00 AM but it captures data at 11:10 AM, then it sends an alert at 11:40 AM onwards based on the alert settings.

Service Level Events	Notification Message
Fluctuations in crypto operations count on a service	Thales Luna Crypto Command Center service monitoring has detected a fluctuation in the operations rate for the following service. > Service Name: <serviceName> > Event Time: <eventCreationTime> > Sensitivity: <sensitivity> std > Type: Immediate **NOTE** 1. A toggle switch is provided for setting the notification for fluctuations in crypto operations count for a service. The CCC administrator can enable the toggle switch to receive notification when there is an instant fluctuation in crypto operations count for a service. 2. A help text is provided to explain this notification setting. 3. It includes a drop down for setting the"**Fluctuations sensitivity**" that can be set only when the notification is enabled. 4. The default value for **"Fluctuations sensitivity"** drop down box is **High = (1 std)**.

Service Level Events	Notification Message
Persistent changes in crypto operations count on a service	Thales Luna Crypto Command Center service monitoring has detected a persistent change in the operations rate for the following service. > Service Name: <serviceName> > Event Time: <eventCreationTime> > Sensitivity: <sensitivity> std > Type: Persists for <persistTime> **NOTE** 1. A toggle switch is provided for setting the notification for persistent fluctuations in crypto operations count for a service. The CCC administrator can enable the toggle switch to receive notification when there is persistent fluctuations in crypto operations count for a service. 2. A help text is provided to explain this notification setting. 3. It includes a drop down for setting the "**Fluctuation sensitivity**" and a drop down for setting the persistent change over a time period and it is labeled as "**Persists for**" . The CCC user can set both these settings only when the notification for persistent fluctuations in crypto operations count on a partition is enabled. 4. The default value for **"Fluctuations sensitivity"** in case of persistent changes is **High = (1 std)** and the default value for **"Persists for"** drop down is **10 minutes**.

Dashboard

This section describes the Dashboard page and tiles. It contains the following topics:

Overview

Only CCC Administrator users can access the **Dashboard**. CCC must be activated and you must have a valid monitoring license to access the **Dashboard**.

The **Dashboard** provides an overview of critical device activity and service availability. It contains device and service tiles which provide details about device and service performance. The **Dashboard** can also be used to quickly access the Device and Service pages. The tiles provide hyperlinks to the relevant page on CCC.

> **NOTE** CCC polls the device monitoring data to populate the **Dashboard**. Device monitoring requires an appliance with REST API. If you monitor a device with firmware lower than 6.20.0 not all monitoring information will be available.

Dashboard Summary

The **Dashboard** provides an overview of CCC device and service functionality. These summary tiles display in the header section of the **Dashboard**.

Device Dashboard Summary

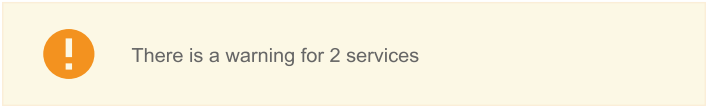
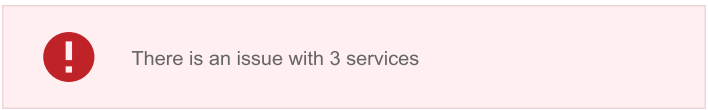
The Dashboard Summary section can contain one of the following device tiles:

 All devices are running without issues	> This tile displays if all devices are running with no issues. > Connects the user to the **Monitoring and Reports** tab. See "Device Monitoring" on page 119 for more information.
 There is an issue with 2 devices	> If there is a problem with any of your devices this tile displays, identifying the number of devices that are not operating properly. > Connects the user to the **Monitoring and Reports** tab. See "Device Monitoring" on page 119 for more information

Service Dashboard Summary

The Dashboard Summary section can contain one of the following service tiles:

 All services are running without issues	> This tile displays if all services are operating with no issues. > Connects the user to the **Services** tab. See "Service Management" on page 84 for more information.

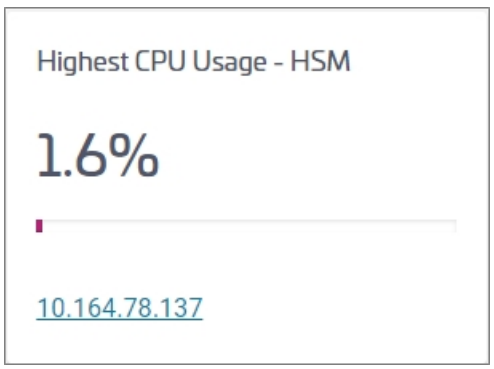
	> This tile displays if there are warnings about any services. > Connects the user to the **Services** tab. See "Service Management" on page 84 for more information.
	> This tile displays if any services are experiencing serious issues. > Connects the user to the **Services** tab. See "Service Management" on page 84 for more information.

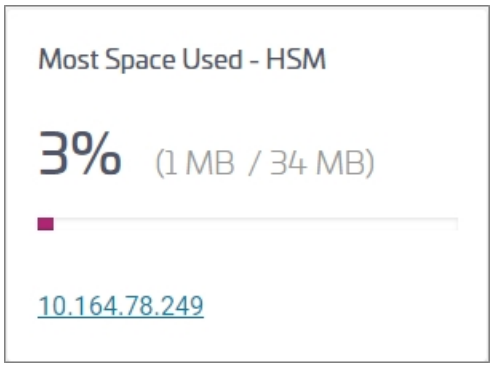
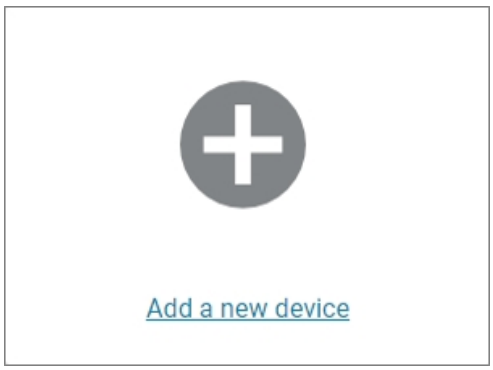
NOTE If there is both a service warning and a service issue, the service tile will display the issue state and message.

NOTE You must add a device to CCC for the **Dashboard** to display the service tiles.

Device Highlights

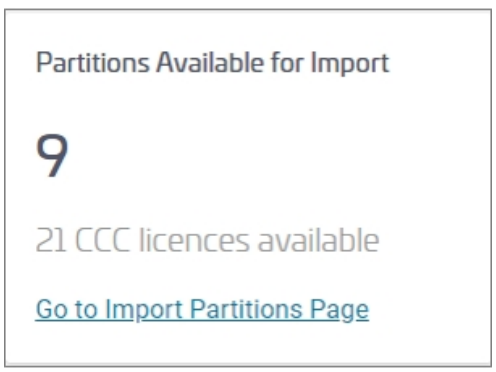
The Device Highlights page contains critical information about device activity and performance. It contains the following device tiles:

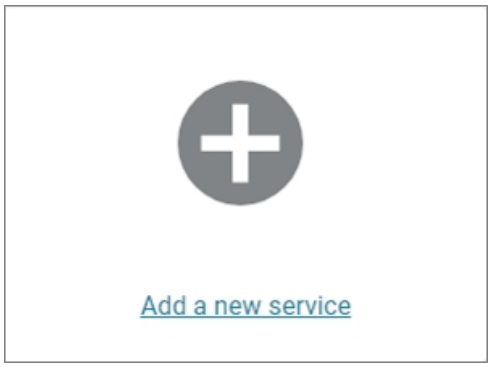
Tile	
	> Displays the device with the highest CPU usage. > Clicking the link takes you to the Device Monitoring page. See "Device Monitoring" on page 119 for more information.

Tile	
	> Displays the device with the most space used. > Clicking the link takes you to the Device Monitoring page. See "Device Monitoring" on page 119for more information.
	> Clicking the **Add a new device** link takes you to the **Add Device** wizard. See "Adding Devices" on page 78 for more information.
View All Devices	Clicking the **View All Devices** link takes you to the **Devices** page. See "Device Management" on page 77 for more information.

Service Highlights

The Service Highlights page contains critical information about service and available cryptographic services. It contains the following service tiles:

Tile	
	> Displays the number of device partitions available for import and the number of available CCC licenses. > Clicking the link takes you to the **Import Partitions** page. See "Discovering and Importing Unmanaged Partitions" on page 87 for more information.

Tile	
	> Clicking the **Add a new service** link takes you to the **Crypto Services** page. See "Service Management" on page 84 for more information.
View All Services	Clicking the **View All Services** link takes you to the **Services** page. See "Service Management" on page 84 for more information.

NOTE You must add a device to CCC for the **Dashboard** to display the service tiles.

Reports

This section describes how to generate reports for the services and devices you manage using CCC. It contains the following sections:

Overview

CCC maintains a record of all currently managed devices, and the services provisioned on those devices. You can use the reporting feature to generate and view reports that provide detailed information for all of your managed devices, or all of your provisioned services. You can view, search, and sort a report in CCC, print it, or export it to a comma separated values (CSV) file you can import into a spreadsheet.

The CSV report contains some additional details not provided in the standard viewable/printable report. See "Exporting a Report to a CSV File" on page 116 for more information.

NOTE CCC polls each of your managed devices to collect the data provided in the report. This may take a significant amount of time.

The report generation functions are grouped under the **Monitoring & Reports** tab if the optional licensed monitoring feature is enabled. See "Device Monitoring" on page 119 for more details.

Services Report

The Services Report provides detailed information about each service managed by CCC. The report includes the following information for each provisioned service:

> the service name

> who created the service, and when it was created

> whether the service is initialized, and who initialized it

> the number of clients assigned to the service

> if service is PPSO and connection link from either NTLS or STC

> the HA group name, if the service is provided by an HA group

> detailed information about the partition(s) used to provide the service, including:

- the partition name(s) and serial number(s)
- the device used to host the partition, including the device name, software version, firmware version, number of clients using the partition, and the client IP addresses

The report also includes unimported partitions of managed devices, displaying a placeholder service name and some partition information.

To generate and view a services report

1. Click on the **Monitoring & Reports** tab, and select **Services Report** in the navigation frame.
2. Click the **Generate Report** button. A report listing all of the currently provisioned services and unimported partitions of managed devices is displayed. The initial view provides the following summary information for each service:

PPSO	Indicates whether the Per-Partition Security Officer feature is enabled or disabled for the service.
Transport	Indicates the transport type configured for client connections to the service, NTLS, STC, or Mismatch. Mismatch indicates that there is a combination of NTLS and STC configuration which should be corrected.
Created By	Name of the user that created the service.
Date Created	Time and date the service was created.
Initialized By	Name of the user that initialized the service.
Initialization State	Indicates whether the service is initialized.
Clients	Number of clients assigned to the partition.
HA Group	Name of the HA group used to provide the service.

3. To view detailed information for each partition used to provide a service, click on the **+** button. The following information is displayed for each partition:

Partition Name	Name of the partition.
PPSO	Indicates whether the Per-Partition Security Officer feature is enabled or disabled for the partition.
Transport	Indicates the transport type configured for client connections to the partition, NTLS or STC. **NOTE** If there is a service which is created on CCC for STC connections, the STC status is "Pending" and the Transport is displayed as "NTLS" until the service is deployed to an application user and the STC link is established.
Serial	Partition serial number.
Device Name	Name of the device that the partition resides on.
Appliance Version	Specifies the software version installed on the device.
Device Firmware	Specifies the firmware version installed on the device.
Clients	Specifies the number of clients assigned to the partition. Not available for partitions with both STC and PPSO configured.
Client List	The IP addresses of the clients assigned to the partition.
STC Fingerprint	A hash of the partition identity public key used to establish STC links.

4. You can search and sort the reports, print them, or export them to a comma separated values (CSV) file for import into a spreadsheet, as described in "Working With Reports" on page 115

NOTE The service report is completed even if there are devices that could not be accessed.

Devices Report

The Devices Report provides the following information for each managed device:

- the device name.
- the software and firmware installed on the device.
- the number of clients authorized to authenticate to the device.
- the total, used and free storage space.
- the maximum allowed number of partitions, and the number of used partitions. These columns are hidden by default.

To generate and view a devices report

1. Click on the **Monitoring & Reports** tab, and select **Devices Report** in the navigation frame.
2. Click the **Generate Report** button. A report listing the following information for each managed device is displayed:

Name	Specifies the device name.
Authentication	Specifies whether the device requires PED or Password authentication.
PPSO	Specifies whether the HSM policy allowing Per-Partition Security Officer is enabled or disabled.
STC	Specifies whether the HSM policy allowing Secure Trusted Channel is enabled or disabled.
Serial	Specifies the serial number of the device.
Appliance Version	Specifies the device software version.
Firmware	Specifies the device firmware version.
Functional Module (FM)	Specifies if the device is FM enabled, disabled or FM incapable.
Clients	Specifies the clients assigned to the partition.
Licenses	Specifies the number of partitions licensed to the device.
Used Space	Specifies the amount of space that is used on the partition.
Size	Specifies the size of the partition.

The following column is hidden by default, but can be displayed as described in "Filtering a Report" on the next page.

Free Space	Specifies the amount of free space on the partition

3. To view detailed information for each managed partition provisioned on the device, click on the **+** button. The following information is displayed for each partition:

Name	Specifies the name of the partition.
PPSO	Indicates whether the partition policy allowing Per-Partition Security Officer is enabled or disabled.

Transport	Indicates whether the partition is configured for NTLS or STC client connections. **NOTE** If there is a service which is created on CCC for STC connections, the STC status is "Pending" and the Transport is displayed as "NTLS" until the service is deployed to an application user and the STC link is established.
Serial	Specifies the partition serial number.
Clients	Specifies the number of clients assigned to the partition.
Client List	Specifies the IP addresses of the clients assigned to the partition.
Object Count	Specifies the number of objects on the partition.
Used Space	Specifies the amount of space that is used on the partition.
STC Fingerprint	A hash of the partition identity public key used to establish STC links.
Size	Specifies the size of the partition.
Free Space	Specifies the amount of free space on the partition.

4. You can search and sort the reports, print them, or export them to a comma separated values (CSV) file for import into a spreadsheet, as described in "Working With Reports" below.

> **NOTE** The device report is completed even if there are devices that could not be accessed.

Working With Reports

You can search and sort the reports, print them, or export them to a comma separated values (CSV) file for import into a spreadsheet.

Searching a Report

You can search a report to filter the list of services or devices to display only matching records. See the User Interface section for more information about searching a report.

Filtering a Report

You can control which columns are displayed in the on screen report. Click on the hamburger menu button on the top right of the report. A list of the columns appears, indicating which columns are currently displayed and which are hidden. Clicking on an individual column changes its states from displayed to hidden, or from hidden to displayed.

Exporting a Report to a CSV File

You can export the report to a comma separated values (CSV) file for import into a spreadsheet. The CSV reports include additional information that is not included in the standard reports, as detailed below.

> **NOTE** CCC polls each of your managed devices to collect the data provided in the report. This may take a significant amount of time.

Information included in the Services report CSV file

The Services report CSV file contains a row for each service managed by CCC. Each row contains the following columns:

name	Service name.
description	Service description.
service_organization	Organization that owns the service.
created_date	Date that the service was created.
created_by	Name of the user who created the service.
initialized_by	Name of the user who initialized the service.
state	Service initialization state. Either INITIALIZED or null.
device_name	Name of the device used to host the partition used to provide the service.
clients	Lists the clients assigned to the partition.
partition_serial_number	Partition serial number. If importing to Excel, format the cell as a number with no decimal places to display the correct serial number.
partition_name	Partition name.
partition_label	Partition label.
partition_size	Partition size.
partition_object_count	The number of objects stored in the partition.
partition_used_space	The used space on the partition.
partition_free_space	The free (unused) space on the partition.
stc_pending_state	Indicates if the STC state is pending for the service, meaning that the STC policy has not yet been enabled on the partition, but will be once an application user establishes an STC connection.

stc	Indicates if the STC policy is enabled on the partition.
ppso	Indicates if the PPSO policy is enabled on the partition.
stc_fingerprint	A hash of the partition identity public key used to establish STC links.

Information included in the Devices report CSV file

The Devices report CSV file contains a row for each partition on each device managed by CCC. Each row contains the following columns:

name	Device name.
description	Device description.
authentication	Device authentication type.
state	Device state.
clients	Clients assigned to the partition.
device_appliance_version	Device software version.
device_firmware_version	Device firmware version.
functionality_Modules	Specifies if the device is FM enabled, disabled or FM incapable.
device_total_space	Total space on the device.
device_total_licenses	The number of partitions licensed on the device.
device_network_replication	The setting of HSM policy 16: Allow Network Replication. 0 = no, 1 = yes.
device_cloning	Whether the device supports cloning. 0 = no, 1 = yes.
device_serial_number	Device serial number. If importing to Excel, format the cell as a number with no decimal places to display the correct serial number.
device_partition_count	The number of partitions currently configured on the device.
device_free_space	Device free space.
service_name	The name of the service configured on the device partition.
service_created_date	The date that the service hosted on the partition was created.
service_created_by	The name of the user who created the service hosted on the partition.

service_initialized_by	The name of the user who initialized the service hosted on the partition, if it is initialized.
service_state	Service initialization state. Either INITIALIZED or null.
partition_serial_number	Partition serial number. If importing to Excel, format the cell as a number with no decimal places to display the correct serial number.
partition_name	Partition name.
partition_label	Partition label.
partition_size	Partition size.
partition_object_count	The number of objects stored in the partition.
partition_used_space	The used space on the partition.
partition_free_space	The free (unused) space on the partition.
stc_pending_state	Indicates if the STC state is pending for the service, meaning that the STC policy has not yet been enabled on the partition, but will be once an application user establishes an STC connection.
stc	Indicates if the STC policy is enabled on the partition.
ppso	Indicates if the PPSO policy is enabled on the partition.
stc_fingerprint	A hash of the partition identity public key used to establish STC links.

To export a report to a CSV file

1. Click on the **Export to CSV** button on the report page. Exporting to CSV requires CCC to poll each of your managed devices to collect the data provided in the report. This may take a significant amount of time. You are asked to confirm the action.
2. When complete, on some browsers, you are prompted to open or save the file, or cancel the action.

> **NOTE** The exported CSV report includes data from both the available and inaccessible devices.
>
> 1. In case of service CSV report, one row is shown for each service and NA is populated in case of specific unknown fields for the services created on non accessible devices.
>
> 2. In case of device CSV report, one row is shown for every specific accessible or non accessible device and NA is populated in case of specific unknown fields.

Printing a Report

You can print the currently displayed report.

To print a report

1. Generate the report.
2. Click on the **Print** button. The browser's print dialog is displayed.
3. Select your print options as required.

Regenerating a Report with More Recent Data

When you generate a report, the data from that time is cached in the browser. Every time you return to one of the Reports pages, the most recent generated report data is displayed. If you would like to regenerate the report with more recent data, you must clear the existing report.

To regenerate a report

1. Navigate to the Device Report or Service Report page.
2. Click on the **Clear** button to delete the current report.

   You are returned to the main Report page.
3. Click the **Generate Report** button.

Device Monitoring

The device monitoring feature generates data displays of managed device information, allowing you to instantly assess the status of all your managed devices, and to view more detailed information for individual devices. For more detailed information about monitored values, consult the *Thales Luna HSM Documentation*.

> **NOTE** Device monitoring requires an appliance with REST API. If you monitor a device with firmware lower than 6.20.0 not all monitoring information will be available.

> **NOTE** Device monitoring is supported for Luna SA 7.4 FM enabled devices.

> **NOTE** The CCC Monitoring feature will require a license that includes monitoring. If the monitoring license is not available, a "**Monitoring license required**" message displays on clicking **Monitoring** in the left navigation frame. Access the Thales Customer Support portal for more information about obtaining a license.

Viewing Monitored Device Information

The main device monitoring table includes columns which provide details on the following:

Status	An indication of device health. Possible values are > Checkmark icon. No problems detected with the device. > Caution icon. The device has a problem which requires attention. > Error icon. Either CCC cannot reach the device or the device has a critical problem preventing it from servicing cryptographic requests.
Name	The name of the device.
Hostname	The Hostname or IP address of the device.
HSM Utilization	A histogram of the HSM utilization percentage for the last 12 checks that CCC has performed. If you sort on this column, the devices appear in ascending order (first sort), or descending order (second sort) of average utilization.
Last Update	Time since the device was last polled.

NOTE The time on Luna SA device should be correct in order to get correct device monitoring information.

You can select an individual device to view more detailed information.

To view history for a device

1. Select the particular device you are interested in.

   The monitored information appears below, in the attributes frame. By default, the History tab is selected.
2. Select the type of data you wish to view as a line chart. Available options are:

History Chart	Description
Crypto Operations - HSM	Charts the number of crypto operations performed per second by the HSM. Crypto operations include: key generation, key derivation, key importing and exporting, random number generation, encryption and decryption services, key signing, and key verification. This allows you to monitor and review high and low crypto operations activity on the HSM.
Operation Requests - HSM	Charts the number of operation requests received per second by the HSM. This allows you to monitor and review high activity operations periods on the HSM.
Non Critical Events - HSM	Charts the number of non critical events on the HSM. Non critical events include: Rest API validation errors, unauthorized requests, failed requests, and forbidden requests. This allows you to monitor non critical incidents on the HSM and identify patterns in their occurrence.

History Chart	Description
Crypto Operation Errors - HSM	Charts the number of crypto operation errors that occur on the HSM. Crypto operations errors can occur during: key generation, key derivation, key importing and exporting, random number generation, encryption and decryption, key signing, and key verification. This allows you to monitor and review the functionality of their HSM.
Commands - HSM	Charts the number of commands input to the HSM. This allows you to monitor and review low and high activity periods for the HSM. **NOTE** The device must be running firmware 6.20.0 or higher in order to display this information.
Critical Events - HSM	Charts the number of critical events which occur per second on the HSM. Critical events include: the HSM losing power, or the HSM stopping operations. This allows you to monitor and identify when critical events occur on the HSM.
Operations Errors - HSM	Charts any operating errors which occur on the HSM operating system. Operations errors include: the operating system disconnecting, or losing power. This allows you to monitor and identify when operations errors occur on the HSM.
CPU Usage - HSM	Charts the percentage of the CPU used by the device. This allows you to monitor the condition of their device CPU. **NOTE** The device must be running firmware 6.20.0 or higher in order to display this information.
Load AVG 1 Minute - Appliance	Charts the average computational work the appliance performs over a 1 minute period.
Load AVG 5 Minutes - Appliance	Charts the average computational work the appliance performs over a 5 minute period.
Load AVG 15 Minutes - Appliance	Charts the average computational work the appliance performs over a 15 minute period.
CPU Temp - Appliance	Charts the temperature of the appliance in degrees Celsius. This allows you to monitor high activity periods and their effect on the internal temperature of the device CPU.
CPU Core Voltage - Appliance	Charts the voltage drawn by the appliance CPU. This allows you to monitor power consumption during high activity periods on the device.

History Chart	Description
Power Supply Temp - Appliance	Charts the temperature of the specified power supply on the appliance in degrees Celsius. This allows you to monitor the condition of the power supply.
Power Supply Voltage - Appliance	Charts the voltage drawn by the specified power supply on the appliance.
Battery Voltage - Appliance	Charts the voltage of the battery connected to the appliance. The battery powers the NVRAM and RTC functions on the device.
Fan Speed - Appliance	Charts the RPM of the specified fan on the appliance. This allows you to monitor the functionality of fans on the device.

By default, the data displayed is for the past hour. You can hover any point on the graph to view a tooltip containing detailed information about that point in time. For example, if you hover over a point in the crypto operations line chart corresponding to 08:00, the number of crypto operations per second that occurred at 08:00 is displayed in text.

3. Select the time period for which you want to view the data.

   The graph updates to show the data trend for the selected time period.

To view appliance data for a device

1. Click the Appliance Data tab.
2. Select the particular device you are interested in.
3. Click Appliance Performance. Information includes the device uptime and the load average for the past 1, 5, and 15 minute(s).
4. View the Hardware Info. There are values for the following:
   - CPU Temperature displayed on a scale of 0 to 120 Degrees Celsius
   - Power Supply Temperatures displayed on a scale of 0 to 120 Degrees Celsius.
   - CPU Voltage displayed on a scale of 0 to 4 Volts.
   - Power Supply Voltages displayed on a scale of 0 to 15 Volts.
   - Battery Voltage displayed on a scale of 0 to 4 Volts.
   - Fan Speeds displayed on a scale of 0 to 10000 revolutions per minute.

     A value of N/A indicates that the device is not returning data.

To view HSM data for a device

> **NOTE** Device monitoring requires an appliance with REST API. The device must be running firmware 6.20.0 or higher in order to display this information.

1. Select the particular device you are interested in.

2. Click the HSM Data tab.
3. View the HSM Performance:
   - The histogram on the right indicates the HSM utilization percentage for the last 12 checks.
   - The Performance indicates whether the HSM is a High or Low performance model.
   - The HSM Utilization indicates the percent utilization of the HSM for the last check.
   - The Operations per Second indicates the number of operations per second the HSM performed since the last check.
4. View the HSM Storage. There are values in kilobytes for maximum storage, used storage, and available storage.
5. View the Partition Information. The Maximum Partitions value indicates the number of partitions you are allowed to create based on the applied maximum partitions capability. The Managed Partitions value indicates the number of partitions currently managed through CCC as services. The used partitions value indicates the number of partitions configured on the CCC. The Partitions Available for Import value indicates the number of partitions which are not imported into CCC.

Event Logs

The Event Logs feature is introduced under Monitoring & Reports tab. It enables export of logs in plain text file format to help in analyzing the different CCC critical events. Administrator users can export three types of logs:

> Monitoring Log
> Server Log
> Operations Log

> **NOTE** The Events Log feature enables administrator users to analyze the exported log files in offline mode.

To export an event log

1. Click on the **Monitoring & Reports** tab, and select **Event Logs** in the navigation frame.
2. The list of logs is displayed in a table that includes columns which provide details on the following:

Log Type	Specifies the type of logs stored in CCC.
Date	Specifies the date when the logs are stored.
Name	Specifies the name of the log files.
Size	Specifies the size of the log files.

> **NOTE**
> 1. The logs list displays all the logs stored in CCC.
> 2. The logs list is paginated and it displays up to 21 logs per page.

3. Click download icon. The download process for that log file starts.

To filter by log type

1. Click **Filter log types**.
2. A drop down menu with three options displays:
   a. Monitoring
   b. Server
   c. Operations
3. Select any of the three options. The logs list is filtered based on the selected option.

Device Logs

You can use the Device Logs feature to export your device logs to a third-party monitoring and analytics tool, and to find and download device logs.

Export Your Device Logs

> **NOTE** To use this feature, you need a monitoring license. If the monitoring license is not available, a “Monitoring license required” message will appear on the screen.

To export device logs to a third-party monitoring and analytics tool, such as Splunk Enterprise:

1. Install Splunk Enterprise on the machine that you want to use for monitoring and analyzing device logs. Follow the installation instructions provided on the Splunk portal:

   https://docs.splunk.com/Documentation/Splunk

2. Install and configure Splunk Universal Forwarder on the same Linux system as the CCC server, using the instructions mentioned on the Splunk portal:

   https://docs.splunk.com/Documentation/Forwarder

3. Execute the following command from the bin directory of Splunk Forwarder:
   a. To monitor all device logs, execute the following command:

   ```
   ./splunk add monitor /usr/safenet/ccc/lunalogs/monitoring/
   ```

   > **NOTE** Executing this command also ensures that any new device that's added starts getting monitored automatically.

   b. To monitor a particular device log, execute the following command:

   ```
   ./splunk add monitor /usr/safenet/ccc/lunalogs/monitoring/<IP address of the device>
   ```

> **NOTE** You can execute this command only when a device has been added and initialized in the CCC server.

Find and Download Device Logs

To find and download device logs:

1. Select a device.
2. Click the **Find Logs** button to view the device logs for the past 30 days, or select a date range and then press the **Find Logs** button to view the device logs for the specified date range.

> **NOTE** You can download Device Logs only for the past 30 days.

3. Download the files that you need.

Notifications

This section describes how to configure notifications. It contains the following topics:

Overview

Administrator users can configure notification messages for critical CCC events. You must have a valid monitoring license to access the **Notifications** page and to configure email notifications.

You can configure a Simple Mail Transfer Protocol (SMTP) server to send event notifications over email from CCC. You can configure notifications for the following events:

> Device is deleted
> Service is deleted
> Connection to a device is lost
> Crypto Command Center is deactivated
> Instant Fluctuations
> Persistent Fluctuations

You must enable email notifications, connect CCC to an SMTP server, add email recipients, and select notification types to configure email notifications from CCC. You can configure notifications from the Monitoring & Reports tab.

See "Notifications" above for more information about enabling or disabling Email Notifications.

See "Configure the SMTP Server Settings" on the next pagefor detailed procedures on configuring and editing and the SMTP Server Settings.

See "Add Email Recipients" on page 128 for Add more information on adding email recipients.

See "Customize Email Notification Types" below for detailed procedures on selecting email notification types.

> **NOTE** In the event that the CCC server goes offline, and the instance becomes deactivated, the notification email will not be sent because the server is not accessible. We recommend using a server monitoring system to monitor the health of the CCC server instances.

Email Notifications

You can enable email notifications to send notification emails for critical CCC events. You can enable or disable notifications from the **Notifications** page on the **Monitoring & Reports** tab.

To enable/disable email notifications

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.

> **NOTE** The CCC Notifications feature will require a license that includes monitoring. If the monitoring license is not available, a "**Monitoring license required**" message displays on clicking **Notifications** in the left navigation frame.

2. Enable or Disable the **Enable email notifications** toggle switch.

Customize Email Notification Types

The CCC Administrator user can define the types of email event notifications. The event email notification is sent to all recipients on the notifications list. The Administrator can enable or disable notifications for the following events:

- Service Level Events
- Device Level Events
- Crypto Command Center Events

Configure the SMTP Server Settings

To send email notifications from CCC you must import the SMTP server settings into CCC. CCC supports all versions of SMTP server.

To configure the SMTP server settings

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.
2. In the email settings section enter the SMTP server information.

Mail Server	Enter the address of the SMTP server. You can enter the address in IP or FQDN format.

Port	Enter the SMTP server port number that CCC will connect to. The default port value for SMTP is 25. Your SMTP server can be configured to use an alternative value. Range: 25, 465, 587,1024 - 65535.
SMTP Username	Enter a valid username that CCC can use to access the SMTP server.
SMTP Password	Enter the password for the provided SMTP username.
Sender Email	Set the sender email address. Ensure that email notifications from CCC are sent from a specific account.
Encryption	Use the drop down menu to select an Encryption type. The Encryption types include: > SSL > TLS

3. Click the **Save Changes** button to save the changes.

> **NOTE** The CCC User can click **Edit Settings** button to modify the changes saved during configuration of SMTP mail server.

To edit the SMTP server settings

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.
2. Select **Edit Settings**.
3. Update the SMTP server information.
4. Click **Save Changes** to update the SMTP configuration, or **Cancel** to close the editor without saving your changes.

To test the connection to the SMTP server

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.

> **NOTE** You must have a configured SMTP server to test the server connection.

2. Select **Edit Settings**.
3. Click the **Test Connection** button.
4. A dialog window displays. Click **Continue** to test the SMTP server configuration, or **Cancel** to close the dialog without testing the SMTP server configuration.

> **NOTE** Testing the email settings may take up to 3 minutes to complete. CCC restricts navigating away from the **Notifications** page during this process.

If the connection is successful a dialog window displays verifying that CCC was able to connect to the SMTP server. If the connection is not successful an error displays identifying the point of failure. The connection error can be one of the following:

Error message	Cause
Connection Failed Could not connect to mail server <host> (No such host is known) Please verify that this information is correct and try again	The host name is incorrect. Verify you have entered the correct information
Connection Failed Could not open connection to <host> on port <port> Please verify that this information is correct and try again	The port number is incorrect. Verify you have entered the correct information.
Connection Failed Incorrect username or password Could not connect to the SMTP server. Please verify that this information is correct and try again	The SMTP username or password is incorrect. Verify you have entered the correct information.
Connection Failed Could not connect to the SMTP server. Please verify that this information is correct and try again	No specific cause is identified.

5. Select **Close** to exit window.

Add Email Recipients

You must add email recipients to the CCC recipients list to send test emails and email notifications from the CCC SMTP server. The test email message is distributed to all users on the recipients list.

You can store up to 100 email addresses in the CCC recipient list. If the recipients list is full the **Add** button will be disabled. If you add the same email address to the list twice, the original entry will be kept and the duplicate will be ignored.

To add email recipients

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.
2. In the **Email Settings** section enter the email address of the intended email recipient in the **Recipient Email Address** field.
3. Press **Enter** or click **Add**.
4. Click the **Save Changes** button to save the changes.

> **NOTE** The CCC User can edit the recipients list by clicking Edit Recipients button.

> **NOTE** To save the SMTP changes, minimum one recipient should be added.

To send a test email message

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.
2. Select **Send Test Email**.
3. A dialog window displays. Click **Continue** to send the test email message, or **Cancel** to close the dialog without sending the test email.

> **NOTE** Sending the test email message may take up to 3 minutes to complete. CCC restricts navigating away from the Notifications page during this process.

> **NOTE** A confirmation message will display if the email message is sent successfully. If the email message fails to send a dialog will open notifying the user of a connection failure.

4. Select **Close** to exit the window.

Service Level Events

It consists of the events occurred at service level.

The service level settings consists of a "**Moving average time period**" drop down with multiple options of time periods that allows the CCC user to choose a time period for sending service alerts on crypto rate fluctuations.

> **NOTE** The different options available for "Moving average time period" are **30 Minutes, 1 hour, 4 hours, 8 hours, 1 day, 3 days, 7 days, 30 days**, and **90 days**.

> **NOTE** A minimum of 30 minutes data is required for a Moving average time period option to send a crypto operation fluctuation alert.

Service Level Events	Notification Message
Fluctuations in crypto operations count on a partition	Thales Luna Crypto Command Center service monitoring has detected a fluctuation in the operations rate for the following service. > Service Name: <serviceName> > Event Time: <eventCreationTime> > Sensitivity: <sensitivity> std > Type: Immediate **NOTE** 1. A toggle switch is provided for setting the notification for fluctuations in crypto operations count on a partition. The CCC user can enable the toggle switch to receive notification when there is an instant fluctuation in crypto operations count on a partition. 2. A help text is provided to explain this notification setting is available with a link for **service monitoring** settings. 3. It includes a drop down for setting the"**Fluctuations sensitivity**" that can be set only when the notification is enabled. 4. The default value for **"Fluctuations sensitivity**" drop down box is **High = (1 std)**.

Service Level Events	Notification Message
Persistent changes in crypto operations count on a partition	Thales Luna Crypto Command Center service monitoring has detected a persistent change in the operations rate for the following service. > Service Name: <serviceName> > Event Time: <eventCreationTime> > Sensitivity: <sensitivity> std > Type: Persists for <persistTime> **NOTE** 1. A toggle switch is provided for setting the notification for persistent fluctuations in crypto operations count on a partition. The CCC user can enable the toggle switch to receive notification when there is persistent fluctuations in crypto operations count on a partition. 2. A help text is provided to explain this notification setting is available with a link for **service monitoring** settings. 3. It includes a drop down for setting the "**Fluctuation sensitivity**" and a drop down for setting the persistent change over a time period and it is labeled as "**Persists for**" . The CCC user can set both these settings only when the notification for persistent fluctuations in crypto operations count on a partition is enabled. 4. The default value for **"Fluctuations sensitivity**" in case of persistent changes is **High = (1 std)** and the default value for **"Persists for"** drop down is **10 minutes**.
Service is deleted	<name_of_service> was deleted from CCC by <user>. **NOTE** A toggle switch is provided for setting the notification for service deletion. The CCC user can enable the toggle switch to receive notification when a service is deleted.

NOTE The Fluctuation sensitivity is used to determine the calculated nth deviation of the standard deviation to specify the range of the data points in which the crypto operations can occur. Thus, 1 std, 2 std, and 3 std denotes the margins of error (or confidence intervals) at different confidence levels.

Device Level Events

It consists of the events occurred at device level.

Device Level Events	Notification Message
Device is deleted	<name_of_device> was deleted from CCC by <user>.
Connection to a device is lost	CCC lost its connection to <name_of_device>. Please log in to restore the connection to this device. See *Troubleshooting Device Connection* in the CCC documentation for more information. **NOTE** A toggle switch is provided for setting the notification for the lost device connection. The CCC user can enable the toggle switch to be notified when a device connection is lost.

Crypto Command Center Events

It consists of the crypto command center events.

Crypto Command Center Events	Notification Message
Crypto Command Center is deactivated	The CCC instance hostname: <hostname> was deactivated. While in the deactivated state all CCC functionality is disabled. To resume functionality an Administrator user must restore the connection to the root-of-trust HSM. See *Root of Trust Activation and Deactivation* in the CCC User Guide for more information. **NOTE** The Crypto Command Center is deactivated email notification is enabled by default.

NOTE In the event that the CCC server goes offline, and the instance becomes deactivated, the notification email will not be sent because the server is not accessible. We recommend using a server monitoring system to monitor the health of the CCC server instances.

To enable or disable event notification types

1. Click on the **Monitoring & Reports** tab, and select **Notifications** in the navigation frame.
2. Enable or disable the corresponding event notification toggle switch.

Support Catalogue

This section describes the Support Catalogue and its important features. It contains the following topics:

> "Overview" on the next page
> "Upload Package" on the next page
> "Apply Package " on page 135

Overview

The Support Catalogue is a tab introduced in CCC to upload a secure package downloaded from the Luna Network HSM support portal. The Support Catalogue is displayed with a white banner underneath the main navigation that displays the support catalogue items and the upload package button on the Support Catalogue page.

> **NOTE** If no secure packages are uploaded to the Support Catalogue, an empty state text displays prompting the CCC administrator to upload secure packages to this page.

Upload Package

The Upload Package feature allows the user to upload a secure package file downloaded from the Luna Network HSM support portal to the Support Catalogue. The package is uploaded to Support Catalogue as a .tar file.

To upload a secure package

1. Navigate to the **Support Catalogue**.
2. Click **Upload Package**. A modal window to upload the package displays.
3. Browse for a **.tar** file to upload.
4. Select the **.tar** file downloaded from the support portal.

> **NOTE** The upload button is disabled until a .tar file is selected. An error message displays if a file type other than .tar is uploaded or the selected file is missing a usable SPKG file or auth file.

5. Click **Upload** to upload the selected **.tar** file.

> **NOTE** If the package is uploaded , an '**Upload successfu**l' message displays. If the package upload fails, an '**Upload failed**' message displays.

To validate checksum of uploaded secure package

1. When the secure package uploads successfully to CCC, a **Verify package** modal window displays.
2. Click the **text box** to enter the checksum retrieved from the Luna Network HSM support portal.
3. Click **Verify**.

> **NOTE** If the checksum value is not entered in the text box, the **Verify** button remains disabled.

4. A verify package indeterminate progress bar displays.

> **NOTE** If the package verification completes, a '**package successfully verified**' message displays.

5. Click **Ok**. An 'Upload successful' modal window displays.
6. Click **Close** to close the modal window.

> **NOTE** If the package verification fails, a **'package verification failed'** message displays.

7. Click **Try Again** to enter a new checksum retrieved from the Luna Network HSM support portal or click **Cancel verification** to abort the package verification.

To cancel uploading a secure package

The user can cancel the uploading of the secure package.

1. Click **Cancel Upload** to abort the upload process. A modal window to cancel the process displays.
2. Click **Yes, Cancel** to cancel the package upload process.
3. Click **No, return to upload** to continue the package upload process.

> **NOTE** If the package upload process is canceled, any artifacts of the uploaded package is deleted from CCC.

To list the uploaded secure packages

User can view the list of uploaded secure packages as tiles on Support Catalogue.

To view the list of uploaded secure packages:

1. Navigate to the Support Catalogue.

The uploaded secure packages are displayed as tiles with following information:

a. Name of the secure package
b. Apply package button
c. View Details button

> **NOTE** All the uploaded secure packages are displayed as tiles on the Support Catalogue page and are sorted by their **upload date** in descending order.

To view details of an uploaded secure package

1. Click **View Details**.

   A Package Details modal window with following information about the uploaded secure package displays:

Name	The name of uploaded secure package.
Uploaded On	The date and time of the uploaded secure package.
Uploaded By	User Email ID.

File size	The file size of the uploaded secure package.
Auth Code	The auth code of the uploaded secure package.
Delete Package	Specifies a button to delete a secure package

You can select an individual device to view more detailed information.

To delete a secure package

1. Click **Delete Package**. A confirmation modal window displays.
2. Click **Delete** to delete the secure package from the CCC server or click **Cancel** to close the confirmation modal window.
3. A **Deleting Package** progress bar displays.

> **NOTE** When the secure package is deleted successfully, a pop up message, "Package successful deleted" displays.

If the secure package deletion fails, an error message displays in a modal window with two options:

a. Try Again

b. Cancel

4. Select **Try Again** to re-initiate the secure package deletion process or **Cancel** to abort the secure package deletion process.

Apply Package

The Apply Package feature allows user to apply a secure package to a device. User can select a device from the device selection list.

The device selection list includes the following details:

Device Name	The name of the device.
Host Name	The Hostname or IP address of the device.
Appliance	The software version of the device.
Firmware	The Firmware of the device.
Serial Number	The serial number of the device.

To apply a secure package

To apply a secure package, following prerequisites are required:

> The device version should be 7.3 or above.

> Rest API version should be 7 or above.

Once the prerequisites are met, following steps are performed to apply a secure package to a device:

1. Click **APPLY PACKAGE**. A modal window displays.

> **NOTE** If the selected secure package is validated, the CCC administrator skips the step number **2, 3,4,5** and proceeds to step number **6** .

> **NOTE** If the selected secure package is not validated, the **Verify package** modal window displays.

2. Copy and paste the checksum retrieved from the Luna Network HSM support portal.
3. Click **Verify** to proceed with checksum verification or click **Cancel** to abort the apply package process.

> **NOTE** The verification continues to check if the secure package downloaded from the support portal is successfully transferred to the Support Catalogue.

4. When the checksum verification completes, the **package successfully verified** message displays.
5. Click **Ok**. The **Select Device** wizard displays.

To select a device and display device info

1. Select a device from the device selection list or **Cancel** to close the modal window without applying the secure package to the selected device.

> **NOTE** To apply a secure package, only one device is selected at a time.

2. Click **Next**.If CCC successfully connects to the device, the **Device Info** wizard displays with the following information:

Host Name	Specifies host name.
Appliance Version	Specifies version of Appliance or device.
Firmware Version	Specifies version of the firmware installed on the device.
Serial No	Specifies serial number of the device.
Partitions List	Specifies list of the partitions available on the device.
Warning Notification	Specifies a message, "Applying a package to this device will temporarily interrupt service to the partitions listed below as well as any unmanaged partitions that are on the device".
Cancel	Specifies a button to close the modal window.
Previous	Specifies a button to return to step 1 of the modal window.

Continue	Specifies a button to display step 3 of the modal window.

> **NOTE** If there are no partitions listed on the device, CCC administrator can proceed with applying the secure package to the device. However, if CCC administrator wants to create a partition before proceeding, you should create a service in the **Crypto Services** tab.

3. If CCC cannot successfully connect to the device, the **Device Info Error** wizard displays with the following information:

Error message	Specifies a message, "Thales Crypto Command Center could not connect to this device".
Cancel	Specifies a button to close the modal window.
Previous	Specifies a button to return to step 1 of the modal window.
Continue	This button is disabled.

> **NOTE**
> 1. If a device is not selected, the **Next** button is disabled.
>
> 2. The user is restricted from performing any actions on CCC GUI during the package update process.
>
> 3. The user can apply the secure package to both PED or Password type devices.

To confirm package application

1. Click **Continue**. A confirmation wizard for package application displays.

   It includes three steps:

   a. Upload package to the device

   b. Verify package and update the device

   c. Reboot the device

2. Type **Proceed**.
3. Click **Apply Package.**
4. The **Upload package to the device** step highlights and a loading bar appears.

   If the secure package upload process fails, an **Upload failed** modal window displays with two options:

   a. Try Again

   b. Cancel Upload

5. Select **Try Again** to re-initiate the upload secure package process or **Cancel Upload** to abort the upload secure package process.

> **NOTE** When user selects **Cancel Upload**, the Upload failed modal window closes and a **red cross (x)** displays with respect to step 1.

If **upload package to the device** completes successfully, a green check displays with respect to step 1.

6. The **verify package and update the device** step highlights and a loading bar appears.

> **NOTE** If verifying and updating the device process fails, an **Update failed** modal window displays and the device remains offline until the verify and update process is re-initiated.

7. Click **Close** to close the Update failed modal window.

> **NOTE** If the verifying and updating the device process completes successfully, a green check displays with respect to step 2.

8. The **Reboot the device** step highlights and a loading bar appears.

> **NOTE** The device is rebooted only if apply a secure package completes successfully.

9. Click **Done** to close the apply package modal window.

When an unknown error occurs in any of the three steps during secure package application to the selected device, a"**Package application failed**" modal window displays and the device remains offline until the secure package update process is re-initiated.

To apply a secure package by adding a device

1. Click **APPLY PACKAGE**. A modal window displays.

   When devices are not available, the modal window displays the following information:

Text	Specifies a message, "There are currently no devices being managed by Crypto Command Center to apply this package to".
Add a device button	Specifies a button to add a device.
Close button	Specifies a button to close the modal window.

2. Click **Add a device** to open **Devices** page and **Add device** modal windowor click **Close** button to close the APPLY PACKAGE modal window.

To update Firmware on a single device

1. Click **Devices** tab. A list of devices displays.

2. Select a device to update firmware. The device information displays.

   In the **General** tab, the **Current Firmware Version** and the **Available Firmware Version Update** options are available.

3. Click **Update to X.X.X** available under **Available Firmware Version Update**. A modal window to update device firmware displays.

> **NOTE** X.X.X is the new firmware version available for update. If there is no firmware version available for update, **No updates available** displays under **Available Firmware Version Update**.

4. Type **Proceed**.
5. Click **Update** to continue the firmware update process or **Cancel** to abort the firmware update process**.**

> **NOTE** When the firmware update process is successful, a confirmation message with a green check displays.

6. Click **Ok**.

If the firmware update process is not successful, a Firmware update failed modal window displays.

7. Click **Close** to close the modal window.

> **NOTE** The firmware upgrade is supported on devices' version 7.2 or above.

CHAPTER 4:
Service Deployment

This chapter describes how Application Owner users deploy services that were created for their organization.

High-level procedure

1. Configure your crypto application server to be used with CCC. See "Configuring Your Crypto Application Server" below.
2. Log in to CCC to view the services created for your organization that are available to be deployed, as described in "Logging Into CCC Center" on the next page.
3. Select the service you want to deploy, and initialize the service if it is not already initialized. See "Initialize" on page 142.
4. Download the CCC Client (**ccc_client.jar**) and copy it to the client workstation where you want to deploy the service. See "Downloading and Installing the CCC Client" on page 144.
5. Run the CCC Client (**ccc_client.jar**) to deploy the service. See "Deploying a Service" on page 145.
6. Begin using the service with your cryptographic applications.
7. Use CCC to revoke access to a service so that it can be re-deployed in the organization, or delete the service if it is no longer required to return the resources used to provide the service to CCC. See "Re-Deploying or Deleting a Service" on page 154.

Configuring Your Crypto Application Server

You must configure your crypto application server to work with CCC before you can deploy a service on it. Configuring your crypto application server involves performing the following tasks:

> installing the Java JDK

> installing the Thales Luna Network HSM client software

Installing the Required Software on the Application Server

Application Owner users of CCC must install the Thales Luna Network HSM client and the Java JDK on any crypto application servers that will use CCC.

To install the required software on a crypto application server

1. Ensure that the Java 1.8 JDK is installed. You must install the full JDK, not just the JRE.
2. Install the Thales Luna Network HSM client. The client version should be at or above the appliance software version installed on the Thales Luna Network HSMs used to provide the services you intend to use. Refer to the *Thales Luna HSM Documentation* for detailed instructions. If you want to use a PED-authenticated service, you must install and configure the Remote PED Server

3. If you want to use a PED-authenticated service you must get an Orange PED key encrypted with the Remote PED Vector (RPV) for the PED-authenticated HSM you want to use. Contact your CCC Administrator for more information.

Logging Into CCC Center

Log into CCC to perform the following tasks:

> view the services created for your organization that are available to be deployed.

> initialize a service. The services may have already been initialized by the CCC Administrator.

> download the CCC Client.

> **NOTE** If the CCC Administrator edits the credentials of a user that has two-factor authentication enabled, the user is required to re-enroll in the two-factor authentication process.

To log in to CCC for the first time

1. Use a supported browser (see Hardware and Software Requirements section) to launch CCC. The URL you use depends on whether the server is identified by IP address or hostname, as follows:
   - **https://**<host_ip>**:8181**
   - **https://**<hostname>**:8181**

   The **Crypto Command Center Login** page is displayed.
2. Log in to the CCC using your Active Directory credentials if you are a directory user, or by using the credentials provided to you by the CCC Administrator if you are a local user.
3. If the Administrator requires that you use two-factor authentication, you are prompted to configure an one time password (OTP). Using a two-factor authentication application on a mobile device, scan the displayed QR code or manually type in the displayed secret key, excluding spaces. Add your account. A 6-digit OTP code is generated. Enter this code into the login page, excluding spaces.

   > **NOTE** The clock for your two-factor authentication application must be synchronized within 2 seconds of the clock for CCC. Otherwise the OTP code will be rejected due to a validation error.

4. You are prompted to change the password in case you are a local user.

To log in to CCC after the first time

1. Use a supported browser (see the Hardware and Software Requirements section) to launch CCC. The URL you use depends on whether the server is identified by IP address or hostname, as follows:
   - **https://**<host_ip>**:8181**
   - **https://**<hostname>**:8181**

   The **Crypto Command Center Login** page is displayed.
2. Log in to the CCC using your credentials. Contact the CCC Administrator if these credentials fail.

3. If you have already configured a one-time password, the application prompts you for the six-digit OTP code. Consult your two-factor application on your mobile device for a current OTP code. Enter this code into the login page, excluding spaces.
4. If your Administrator has added the requirement for two-factor authentication or the secret key has been reset since your last login, a QR code and secret key are displayed. Using a two-factor authentication application on a mobile device, scan the displayed QR code or manually type in the displayed secret key, excluding spaces. Add your account. A 6-digit OTP code is generated. Enter this code into the login page, excluding spaces.

> **NOTE** The clock for your two-factor authentication application must be synchronized within 2 seconds of the clock for CCC. Otherwise the OTP code will be rejected due to a validation error.

Initialize

Viewing and Initializing Services.

After you log in to CCC, a list of the services created for your organization that are available to be deployed is displayed. The list includes the service name and its initialization state. Services may have already been initialized by the CCC Administrator, or they may be awaiting initialization. A service must be initialized before it can be deployed.

Viewing Service Attributes

Click on a service to display its attributes at the bottom of the page. To help find a service, you can sort the service list by column heading, or use the search function.

To view the attributes for a service

1. Click on **Services** in the navigation frame to display a list of all added services.
2. After finding the service you want to view, click on the service to display its attributes.
3. Click on a tab to view the service attributes, as follows:

General	Displays the service name, description, and organization. Click **Edit** to change the name or description. This information is used to identify the device in CCC.
Capabilities	Displays the service type, partition size, authentication type, and the capabilities of the host device.
Partitions	Displays the name(s) and serial number(s) of the partition(s) that provide the service, if the service is initialized.
Keys	Displays the Label, Type, Handle, Fingerprint, Algorithm, and Bit Size of the keys present on partitions associated with a service.

Clients	Displays the host name of the Thales Luna HSM client workstation that the service is deployed on, if it is deployed.

Initializing a Service

You must initialize a service before you can register it with your application server and begin using it with your applications. Initializing a service initializes the partition(s) used to provide the service on the host device(s). CCC Admin users can initialize a service when they create it, or they can leave it uninitialized until it is ready to be deployed. Uninitialized services can be initialized by the CCC Administrator, or by an Application Owner that is a member of the organization that owns the service.

To initialize a service, you must specify or create the following:

> the initial credentials for the roles that will own or use the service:
  - for services without PPSO enabled, you initialize the credentials for the partition owner (crypto officer) role.
  - for services with PPSO enabled, you initialize the credentials for the partition SO and crypto officer roles. You also have the option to initialize the crypto user role.

> the cloning domain for the service. You can only clone objects between HSMs that are in the same cloning domain. Cloning is used to perform operations such as backup/restore.

To initialize a password-authenticated service

1. Click on **Services** in the navigation frame to display a list of the services created for your organization that are available to be deployed. Any uninitialized services have an Initialize link in the Initialization State column. To help find a service, you can sort the service list by column heading, or use the search function.
2. After finding the service you want, click on the **Initialize** link in the **Initialization State** column. The **Initialize Service** wizard is displayed. Complete the wizard as follows:

Define Partition	Enter a label and cloning domain for the partition used to provide the service.
Initialize Roles	Set the initial password for the crypto officer. For PPSO services, you also set the initial password for the partition security officer, and optionally for the crypto user. Click **Finish** to initialize the service. Observe the progress messages to verify success. **NOTE** For a service which used STC and PPSO, after the service is deployed you cannot initialize the Crypto User role through CCC.

3. Click the **Finish** button to initialize the service.

To initialize a PED-authenticated service

You require a remote PED to initialize a PED-based service. To use a remote PED with CCC you must do the following:

> Install the Thales Luna HSM client, including the remote PED server option, on the computer you will use to access CCC, or on a separate computer you will use for the remote PED.

> Configure the Remote PED Server on the computer you will use for the remote PED. Refer to the *Thales Luna HSM documentation* for more information.

> Get an orange PED key encoded with the Remote PED Vector (RPV) for the Thales Luna Network HSM appliance that provides the service. Contact the CCC Administrator to get the key.

1. Click on **Crypto Services** in the navigation frame to display a list of the services created for your organization that are available to be deployed. Any uninitialized services have an Initialize link in the Initialization State column. To help find a service, you can sort the service list by column heading, or use the search function.
2. After finding the service you want, click on the **Initialize** link in the **Initialization State** column. The **Initialize Service** dialog is displayed. Complete the dialog as follows:

Define Partition	Enter a label for the partition used to provide the service.
Initialize Roles	Enter the IP address of your remote PED server. The default port is auto-filled. If you are not using the default port, enter the Remote PED server port. For PPSO services, enter the challenge password for the crypto officer and (optionally) crypto user roles. The challenge password is the password used to authenticate to the role after it is activated. Click **Next** and respond to the prompts on-screen and on the PED. For non-PPSO services, the PED generates and displays a 16-digit challenge password. Record this challenge password. It is necessary for service activation.
Activate Roles	To activate the roles you initialized, click the **Activate Crypto Officer** and (optionally) **Activate Crypto User** checkboxes. You cannot activate the Crypto User without also activating the Crypto Officer. You can activate the roles later, if desired, by editing the service attributes. For services which have the both the Per-Partition Security Officer and the Secure Trusted Channel feature enabled in the template, you can activate the roles any time until an application user deploys the service, which establishes the STC link and precludes further changes through CCC. Otherwise you can activate the roles at any time. Click **Finish** to initialize the service. Observe the progress messages to verify success.

Downloading and Installing the CCC Client

The CCC client must be installed in the same directory as the Thales Luna HSM client binaries on the crypto application server where you want to deploy a service. You can download the client directly to the crypto application server, or you can download it to another workstation and copy it to the crypto application server.

To download and install the CCC client

1. Log in to CCC, as described in "Logging Into CCC Center" on page 141.
2. Click on **Software Center** to display a list of software available for download.
3. Click on the **Download Crypto Command Center Client** link to download the client software (**ccc_client.jar**).

4. Copy **ccc_client.jar** to the same directory as the Thales Luna HSM client binaries on the crypto application server where you want to deploy a service.

Linux	/usr/safenet/lunaclient/bin
Windows	C:\Program Files\SafeNet\LunaClient\

Deploying a Service

This section describes how to perform tasks related to deploying a service on a crypto application server. It contains the following sections:

Overview

After you have initialized a service using CCC, you need to run the CCC Client (**ccc_client.jar**) from your crypto application server to register your client with the HSM used to host the service before you can begin to use the service. When you run **ccc_client.jar**, it automatically creates an NTLS or STC connection between your crypto application server and the device(s) associated with the service. The connection is NTLS unless the service configuration indicates that the STC should be enabled on the device partition(s). You can view the STC status for a service in the capabilities tab, as described in "Initialize" on page 142.

The only information you require is the CCC hostname, IP address, or fully qualified domain name, your CCC username, and for services that use both STC and Per-Partition Security Officer (PPSO), the partition officer credentials. The fully qualified domain name is preferred, as that value is recommended for the common name of the server certificate to prevent IP address conflicts in high availability configurations. If you wish to specify an IP address or hostname, contact the CCC Administrator to regenerate the certificate using IP address in the subjectAltName field.

If you have multiple deployed and initialized services awaiting registration, **ccc_client.jar** presents a list of the available services, from which you can select the service you want to register.

Using the CCC Client to Deploy an NTLS Service

After you download and install the CCC Client to your crypto application server, you can use it to deploy services on the workstation. Go to "Using the CCC to Deploy an STC Service" on page 148 if you wish to deploy a service configured for STC transport.

> **NOTE** The option to support the "Repair Client" feature for PPSO-STC partially initialized services is not available.

To deploy a service

1. Run these commands using sudo (Linux) or launch an Administrator command prompt (Windows) on the crypto application server that will use the service.
2. Go to the directory where **ccc_client.jar** is installed:

Linux	cd /usr/safenet/lunaclient/bin
Windows	C:\Program Files\SafeNet\LunaClient\

3. Run **ccc_client.jar**:

   java -jar ccc_client.jar -user <username> [**-password** <password>] [**-otp** <otp code> **-host** <CCC_server_hostname_or_IP> [**-port** <CCC_server_port>]

   If you specify a password as part of the command, enclose it in single quotation marks (in Linux, as in the example), or double quotation marks (in Windows). If you do not specify a password, you are prompted for one, in which case do not use quotation marks.

   If your account has one-time password (OTP) configured, you must either include the **-otp** parameter, or respond when prompted for the one-time password code. Consult your two-factor application on your mobile device for a current OTP code. Enter the six digit code with no spaces.

   The **-port** parameter is optional. If not specified, the default port 8181 is used.

   For example:

   ```
   java -jar ccc_client.jar -user myname@myorg -password 'mypassword' -host cccserver
   ```

4. You are prompted to accept the CCC server certificate. This message is not displayed if you previously imported the certificate on this client:

   ```
   Connecting ...
   Server certificate is not trusted.
   Select one of the following options to proceed:
   1: Show the certificate details
   2: Trust the certificate this time only
   3: Trust the certificate and permanently import it to the trusted keystore at:
      C:\Program Files\Java\jre8\lib\security\cacerts
   4: Exit
   Enter an option(1-4):
   ```

   Enter **1** to display the certificate.

   Enter **2** to trust the certificate for this deployment only.

   Enter **3** to permanently trust the certificate.

   Enter **4** to exit the client without deploying the service.

5. A client certificate for NTLS connections to service partitions is created, if the certificate is not present. You are prompted for an IP or hostname to register with partitions.

   ```
   Creating certificate...
   Please choose the IP address or hostname you want to register with HSMs
   1) 1.1.1.1
   2) 192.168.1.1
   3) Manually enter a different IP or hostname
   Option: 1
   ```

6. If you choose to permanantly trust the certificate, you are prompted to enter the trusted keystore password:

```
Enter the trusted keystore password:
```

   Enter the trusted keystore password for the Java JDK installed on the Thales Luna HSM client workstation. The default password is **changeit**.

7. A list of the services created for your organization that are available to be deployed are displayed. Select the service you want to authorize your client to use.

```
Logging in ...
Querying current services...
Please select the service you want to configure:
1) Service_with_a_smile - No description
2) Now_thats_service - Password partition
3) Self_service - PED HA group
4) Exit
```

8. You are prompted to authorize, revoke, or repair access. Select option 1 to authorize access.

```
Please select the action you want to execute:
1) Authorize Access
2) Repair Access
3) Revoke Access
4) Exit
Option: 1
```

> **NOTE** When a partition is added or removed from an existing service, the CCC application owner can use "Repair Access" option to create a NTLS link with new service partition added to the client's HA group.

9. If you are authorizing a PED-authenticated HSM Partition HA Group service, go to the next step. Otherwise, the following message is displayed:

```
Would you like to authorize access to service 'Service_with_a_smile'? (Y/N): y
Access to service 'Service_with_a_smile' was successfully granted.
Done
```

   The procedure is complete.

10. For PED-authenticated HSM Partition HA Group services, the service cannot be authorized until each partition in the HA group has been assigned the same challenge password and has been activated. If the HA group has the Per-Partition Security Officer (PPSO) feature enabled, you can activate through the CCC user interface, as described in "Service Management" on page 84. If PPSO is not enabled, continue in this section. This task can be performed by the Administrator when creating the service, or by the Application Owner when deploying the service. When you attempt to authorize the service, the following message is displayed:

```
Would you like to authorize access to service 'Self_service'? (Y/N): y
Configuring HSM Partition HA group...
List of group members:
label: partition-00 (serial number: 111111111110)
label: partition-01 (serial number: 111111111111)

Have you manually changed the challenges for the 'HAGROUP' group members? (Y/N):
```

- If you are sure that each partition in the HA group has been assigned the same challenge password, enter **y**. You are prompted to enter the challenge password:

  ```
  Enter the group challenge for group HAGROUP:
  ```

  Enter the challenge password. If successful, the following message is displayed:

  ```
  Access to service 'Self_service' was successfully granted.
  ```

  If not successful, an error indicating that the challenge passwords do not match is displayed. In this case, re-run **ccc_client.jar**, answer **n** to the challenge passwords prompt, and complete this procedure for the case when you have not manually changed the challenges for the HA group members.

  > **NOTE** This error is displayed if either the passwords do not match, or if the partitions are not activated.

- If you have not assigned the same challenge password to each partition in the HA group, enter **n**. The following prompt is displayed.

  ```
  Process paused.  If you wish to align the CO challenges and activate the CO roles now, open
   a new console and run LunaCM to perform these operations.  Once you have done so, select
   "Continue" below to proceed with this HA Group configuration.
  1. Continue
  2. Exit
  ```

  Set the challenge password for each listed member, as described in "Activating a non-PPSO PED-Authenticated HA Group" on page 151.

Using the CCC to Deploy an STC Service

STC services are deployed slightly differently than NTLS services because of the need to exchange client identity and partition identity public keys.

If the service was imported into CCC, and had both the STC and Per-Partition Security Officer policies enabled before import, you cannot deploy the service. This is because the Partition SO can only access and modify the partition through the existing STC client that was established before import.

To deploy a STC service

1. If you are using a hard token, initialize it in a Windows computer as described in Thales Luna HSM documentation.
2. Run these commands using sudo (Linux) or launch an Administrator command prompt (Windows) on the crypto application server that will use the service.
3. Go to the directory where **ccc_client.jar** is installed:

Linux	cd /usr/safenet/lunaclient/bin
Windows	C:\Program Files\SafeNet\LunaClient\

4. Run **ccc_client.jar**:

   java -jar ccc_client.jar -user <username> [**-password** <password>] [**-otp** <otp code>] **-host** <CCC_server_hostname_or_IP> [**-port** <CCC_server_port>]

If you specify a password as part of the command, enclose it in single quotation marks (for Linux, as in the example) or double quotation marks (for Windows). If you do not specify a password, you are prompted for one, in which case do not use quotation marks.

If your account has one-time password (OTP) configured, you must either include the **-otp** parameter, or respond when prompted for the one-time password code. Consult your two-factor application on your mobile device for a current OTP code. Enter the six digit code with no spaces.

The **-port** parameter is optional. If not specified, the default port 8181 is used.

For example:

```
java -jar ccc_client.jar -user myname@myorg -password 'mypassword' -host cccserver
```

5. You are prompted to accept the CCC server certificate. This message is not displayed if you previously imported the certificate on this client:

```
Connecting ...
Server certificate is not trusted.
Select one of the following options to proceed:
1: Show the certificate details
2: Trust the certificate this time only
3: Trust the certificate and permanently import it to the trusted keystore at:
   C:\Program Files\Java\jre8\lib\security\cacerts
4: Exit
Enter an option(1-4):
```

   Enter **1** to display the certificate.

   Enter **2** to trust the certificate for this deployment only.

   Enter **3** to permanently trust the certificate.

   Enter **4** to exit the client without deploying the service.

6. A client certificate for NTLS connections to service partitions is created, if the certificate is not present. You are prompted for an IP or hostname to register with partitions.

```
Creating certificate...
Please choose the IP address or hostname you want to register with HSMs
1) 1.1.1.1
2) 192.168.1.1
3) Manually enter a different IP or hostname
Option: 1
```

7. If you choose to permanantly trust the certificate, you are prompted to enter the trusted keystore password:

```
Enter the trusted keystore password:
```

   Enter the trusted keystore password for the Java JDK installed on the Thales Luna HSM client workstation. The default password is **changeit**.

8. A list of the services created for your organization that are available to be deployed are displayed. Select the service you want to authorize your client to use.

```
Logging in ...
Querying current services...
Please select the service you want to configure:
1) Service_with_a_smile - No description
2) Now_thats_service - Password partition
```

```
3) Self_service - PED HA group
4) Exit
```

9. You are prompted to authorize access. Select option 1 to authorize access.

```
Please select the action you want to execute:
1) Authorize STC Access
2) Exit
Option: 1
```

> **NOTE** If your service uses STC and Per-Partition SO together, CCC cannot revoke STC access and the option is not available. This prevents the risk of leaving the partition (s) with no client connections, which would make partition access unrecoverable. See "Re-Deploying or Deleting a Service" on page 154 for more details.

10. If no STC client ID is found on the application server, you are prompted to create one. Enter Y and enter a desired Client Name to be registered on the partition(s).

```
STC Client ID not found.  Do you want to create one? (Y/N): y
Enter the STC Client Name: CCC_Application_1
```

11. If the device has the PPSO feature enabled, you are prompted for the Partition SO credentials to create the connection.

```
Configuring STC connection...
```

- For password authenticated devices, you are prompted for the PSO password.

  ```
  Enter PSO Password:
  ```

- For PED authenticated devices, you are prompted for the Remote PED IP and port. The remote PED prompts you for the orange Remote PED key, and the blue Partition Security Officer key.

  ```
  Enter Remote PED IP Address:
  Enter Remote PED Port:
  ```

12. The STC client ID label is displayed. This could be an STC client ID created in step 10, or outside of ccc_ client. You are given the option to change the client label registered on the partition(s).

```
STC Client will be registered with the client label 'ExistingName' on service 'Service_with_a_
smile'.
Do you wish to change the registered STC Client Label? (Y/N): n
```

If you are authorizing a PED-authenticated HSM Partition HA Group service, go to the next step. Otherwise, the procedure is complete.

13. For PED-authenticated HSM Partition HA Group services, the service cannot be authorized until each partition in the HA group has been assigned the same challenge password and has been activated. If the HA group has the Per-Partition Security Officer (PPSO) feature enabled, you can activate through the CCC user interface, as described "Service Management" on page 84. If PPSO is not enabled, continue in this section. When you attempt to authorize the service, the following message is displayed:

```
Would you like to authorize access to service 'Self_service'? (Y/N): y
Configuring HSM Partition HA group...
List of group members:
label: partition-00 (serial number: 111111111110)
label: partition-01 (serial number: 111111111111)
Have you manually changed the challenges for the 'HAGROUP' group members? (Y/N):
```

- If you are sure that each partition in the HA group has been assigned the same challenge password, enter **y**. You are prompted to enter the challenge password:

  ```
  Enter the group challenge for group HAGROUP:
  ```

  Enter the password. If successful, the following message is displayed:

  ```
  Access to service 'Self_service' was successfully granted.
  ```

  If not successful, an error indicating that the challenge passwords do not match is displayed. In this case, re-run **ccc_client.jar**, answer **n** to the challenge passwords prompt, and complete this procedure for the case when you have not manually changed the challenges for the HA group members.

  > **NOTE** This error is displayed if either the passwords do not match, or if the partitions are not activated.

- If you have not assigned the same challenge password to each partition in the HA group, enter **n**. The following prompt is displayed.

  ```
  Process paused.  If you wish to align the CO challenges and activate the CO roles now, open
   a new console and run LunaCM to perform these operations.  Once you have done so, select
   "Continue" below to proceed with this HA Group configuration.
  1. Continue
  2. Exit
  ```

  Set the challenge password for each listed member, as described in "Activating a non-PPSO PED-Authenticated HA Group" below

Activating a non-PPSO PED-Authenticated HA Group

To successfully authorize access to a PED-authenticated HSM Partition HA Group, each partition in the HA group must use the same challenge password, and be activated. If the HA group does not have PPSO enabled, perform the following procedure to activate.

Prerequisites

You require:

> the 16-digit challenge password generated by the PED when the service was initialized.

> the partition owner/crypto officer (black) PED key.

> **NOTE** If the user enters an incorrect challenge password when deploying a PED-authenticated HSM partition HA group service with ccc_client, the service will display as deployed but will not be operational. To deploy the service, re-launch ccc_client, select the service, and revoke access to that service. Then, deploy the service as described in the *CCC User Guide*.

To set the challenge password and activate a non-PPSO PED-authenticated HA group member

1. Run **ccc_client.jar** and proceed till you see the following prompt:

   ```
   Enter the group challenge for group <group_name>:
   ```

At this point each member of the HSM Partition HA Group service will be available as a slot in LunaCM.

2. Open a Thales Luna HSM client session:
   a. Open a command prompt or terminal window.
   b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\bin\lunacm
Linux/AIX	/usr/safenet/lunaclient/data/bin/lunacm
Solaris/HP-UX	/opt/safenet/lunaclient/data/bin/lunacm

3. Display a list of the available slots and note the firmware versions. If the partitions have firmware version 6.22 or higher (which was released alongside software version 6.0) **role** commands are required in LunaCM for the rest of this procedure. If the partitions have firmware below 6.22, **partition** commands are required in LunaCM.

   lunacm:> **slot list**

4. Set the current slot to a slot containing one of the HSM Partition HA Group members:

   lunacm:> **slot set -slot** <slot_number>

5. Connect the PED to your remote PED server:

   lunacm:> **ped connect -ip** <remote_ped_server_IP>

6. If the devices are firmware version 6.22 or above, skip to step 7. If the devices are below firmware version 6.22, do the following:
   a. Log in to the partition. You are prompted to attend to the PED to provide the orange (remote PED) and black (Partition Owner/Crypto Officer) PED keys:

      lunacm:> **partition login**

   b. Set the challenge password for the partition:

   lunacm:> **partition changepw -p**

   For example:

```
lunacm:> partition changepw -p

Option -oldpw was not supplied. It is required.

Enter the old challenge: ***********
```

   The old challenge password is displayed on the PED.

```
Option -newpw was not supplied. It is required.
Enter the new challenge: ***********
Re-enter the new password: ***********
User is not activated, please attend to the PED.

Command Result : No Error
```

   c. Log out of the partition:

      lunacm:> **partition logout**

d. Log in to the partition. You are prompted to attend to the PED:

   lunacm:> **partition login**

e. Activate the partition:

   lunacm:> **partition activate**

   For example:

```
lunacm:> partition activate

Option -password was not supplied. It is required.
Enter the password: ****************
User is not activated, please attend to the PED.

Command Result : No Error
```

f. Repeat a-e for every partition in the HSM Partition HA Group. Go to step 8.

7. If your devices are firmware version 6.22 or above, do the following:

   a. Activate the Crypto Officer role by logging it in.

      lunacm:> **role login -name Crypto Officer**

      The PED prompts you for the black PED key.

   b. Change the role's challenge password .

      lunacm: **role changePW -name Crypto Officer -old <oldpassword> -new <newpassword>**

   c. If you expect the Crypto User to be using the service regularly, log that role in and change its challenge password.

      lunacm:> **role login -name Crypto User**

      lunacm: **role changePW -name Crypto User -old <oldpassword> -new <newpassword>**

      You are prompted for the Crypto User PED key.

   d. Once you entered the Crypto User PED key, logout the role.

      lunacm:> **role logout**

      Repeat a-d for every partition in the HSM HA Group.

8. Disconnect the remote PED:

   lunacm:> **ped disconnect**

9. Return to the **ccc_client.jar** session and enter the group challenge to continue and complete the service deployment.

Accessing the Service

After you authorize your client to access a service, you can use the service to run client applications, such as ckdemo, multitoken, or your own custom applications.

If the service is provided by a PED-authenticated, FIPS Level 3 device, you must log into the device using a PED and a black PED key before you can begin using the service. You will need to present the black PED key each time you use the service to run a client application, unless you activate the partition that provides the service. Partition activation eliminates the need to present the black PED key each time you use the service, by

allowing you to log in to the activated partition using a password. You can use the LunaCM utility to activate a partition only if the activation policy for the partition is set to on. Refer to the Thales Luna HSM documentation for details.

> **NOTE** You cannot use CCC to log in, change partition policies, or activate partitions on devices that do not have the REST API enabled. You must use the Thales Luna HSM Client utilities to perform these tasks.

Re-Deploying or Deleting a Service

This section describes how to revoke access to a service so that it can be re-deployed, or delete a service if it is no longer required. It contains the following sections:

> "Overview" below

> "Revoking Access to a Service" below

> "Deleting a Service" on page 156

Overview

When you are done using an HSM service, you can use the CCC client to revoke access to the service. If your organization no longer requires the service, you can delete the service to make the resources used to provide the service available to the CCC Administrator to create new services.

Revoking Access to a Service

When you revoke access to a service, the service is de-registered and the NTLS or STC link is taken down, so that the slot for the service is no longer available to the Thales Luna HSM client.

> **NOTE** If your service uses STC and Per-Partition SO together, CCC cannot revoke access. The Partition SO must manage STC client revocation through LunaCM. This method prevents the risk of leaving the partition(s) with no client connections, which would make partition access unrecoverable.

To revoke access to an HSM service

1. Run these commands using sudo (Linux) or launch an Administrator command prompt (Windows) on the crypto application server that will use the service.
2. Go to the directory where **ccc_client.jar** is installed:

Linux	cd /usr/safenet/lunaclient/bin
Windows	C:\Program Files\SafeNet\LunaClient\

3. Run **ccc_client.jar**:

   java -jar ccc_client.jar -user <username> [**-password** <password>] **-host** <CCC_server_hostname_or_IP> [**-port** <CCC_server_port>]

The **-port** parameter is optional. If not specified, the default port 8181 is used.

For example:

```
java -jar ccc_client.jar -user myname@myorg -host cccserver
```

4. You are prompted to accept the CCC server certificate. This message is not displayed if you previously imported the certificate on this client:

```
Connecting ...
Server certificate is not trusted.
Select one of the following options to proceed:
1: Show the certificate details
2: Trust the certificate this time only
3: Trust the certificate and permanently import it to the trusted keystore at:
   C:\Program Files\Java\jre8\lib\security\cacerts
4: Exit
Enter an option(1-4):
```

Enter **1** to display the certificate.

Enter **2** to trust the certificate for this deployment only.

Enter **3** to permanently trust the certificate.

Enter **4** to exit the client without deploying the service.

5. You are prompted to enter the trusted keystore password:

```
Enter the trusted keystore password:
```

Enter the trusted keystore password for the Java JDK installed on the Thales Luna HSM client workstation. The default password is **changeit**.

6. A list of the services created for your organization, that are available to be deployed, are displayed. Select the service you want to revoke access to.

```
Logging in ...
Querying current services...
Please select the service you want to configure:
1) Service_with_a_smile - No description
2) Now_thats_service - Password
3) Self_service - PED
4) Exit
```

7. You are prompted to authorize or revoke access. Select option 3 to revoke access.

```
Please select the action you want to execute:
1) Authorize Access
2) Repair Access
3) Revoke Access
4) Exit
Option: 3
```

8. You are prompted to confirm the action.

```
Would you like to revoke access to service 'Service_with_a_smile'? (Y/N): y
Access to service 'Service_with_a_smile' was successfully revoked.
Done
```

Deleting a Service

When you delete a service, the resources used to provide the service are returned to CCC.

To delete a service

You can delete a service from CCC if it is no longer required.

> ****WARNING** Deleting a service deletes the partition(s) used to provide the service and all objects in the partition(s).**

1. Log in to CCC. See "Logging Into CCC Center" on page 141.
1. Select **Services** in the navigation frame.
2. After finding the service you want, click on the **trash can icon** in the **Delete** column. A confirmation dialog is displayed.

APPENDIX A: Troubleshooting

The following sections provide solutions, workarounds, and explanations about issues that you might encounter as you deploy CCC:

Browser Issues

I'm unable to access CCC on Mozilla Firefox even after I click the Accept the risk and continue button

This issue is specific to Mozilla Firefox. You can either access CCC on Google Chrome or Microsoft Edge, or follow these steps to access CCC on Mozilla Firefox:

1. Click the **Options** tab from the menu on the right.
2. Click **Privacy and Security** option from the navigation pane on left and then scroll down to the **Certificates** section.
3. Click the **View Certificates** button and then click the **Servers** tab from the **Security Manager** window that appears on the screen.
4. Click **Add Exception** button at the bottom.
5. Enter the CCC path in the **Add Security Exception** window that appears on the screen.
6. Click the **Get Certificate** button and then click the **Confirm Security Exception** button after the certificate gets generated.

You should now be able to access CCC on Mozilla Firefox.

Installation Issues

How can I resolve the following error that I'm encountering when I run the sh install.sh –check command: "This script must be executed by root privilege"

To overcome this issue, you need to log in as the root user.

How can I resolve the following error that I'm encountering during the CCC installation: "Perl command not installed"
To resolve this issue, you need to install Perl using the following command: `yum install perl`.

How can I resolve the following error that I'm encountering during the CCC installation: "[Error] openssl command not installed"
To resolve this issue, you need to install OpenSSL using the following command: `yum install openssl`

Configuration Issues

I'm encountering an error while configuring CCC
Run the `sh config.sh –debug` command to see a detailed error log on your screen. Based on the error that is displayed in the error log, you can make the necessary changes and then run the `sh config.sh` command again. In case you are not able to resolve the issue using the error log, take a screenshot of the error log and contact Thales Customer Support.

I'm encountering the following error when I run the sh config.sh –check command: "This script must be executed by root privilege"
To resolve this issue, you need to log in as the root user.

I'm encountering the following error during the CCC configuration: "[Error] User lunadirector does not exist"
To resolve this error, you need to re-install CCC.

I'm encountering the following error during CCC configuration: "[Error] ipcalc command not installed"
To resolve this error, you need to install ipcalc using the following command: `yum install initscripts`.

I'm encountering the following error during CCC configuration: "[Error] JCPROV_HOME is not defined"
To resolve this error, you need to check whether lunaclient has been installed properly.

I'm encountering the following error during CCC configuration: "[Error] JCPROV libraries not found. Please make sure you have LunaClient with JCProv installed on this machine"
To resolve this error, you need to check whether lunaclient has been installed properly.

I'm encountering the following database connection error at the time of configuration: "Server chose TLSv1, but that protocol version is not enabled or supported by the client" or "Server chose TLSv1.1, but that protocol version is not enabled or supported by the client"
If you are using a CentOS 8 or RHEL 8 operating system, you may get this error at the time of CCC configuration. This is because CentOS 8 and RHEL 8 have deprecated TLSv1.0 and TLSv1.1. To overcome this issue, either upgrade database TLS version to TLSv1.2 or above, or change policy on CCC server by running the `update-crypto-policies --set LEGACY` command.

After re-configuring CCC, the server starts successfully but the CCC URL lands on a blank page
This can be a result of configuration mismatch between the CCC and database. During CCC configuration, if you enter “no” in response to the message “The CCC database is already configured. Do you want to change the database configuration?”, ensure that the current configuration properties of the database are aligned with the previous settings. If there is any change in database configuration, enter “yes” in response to the above-stated message and then re-configure CCC with new database settings.

Administration Issues

I'm encountering the following message while activating CCC root of trust: "System already activated"
To resolve this issue, you need to:

1. Activate the ROT again by entering the partition label and password.
2. Check the **Remember credentials** checkbox if you want CCC to cache your root of trust credentials.
3. Click the **Activate** button.

Uninstallation Issues

I’m encountering an error while uninstalling CCC
Run the `sh uninstall.sh -debug` command to see a detailed error log on your screen. Based on the error that is displayed in the error log, you can make the necessary changes and then run the `sh uninstall.sh` command again. In case you are not able to resolve the issue using the error log, take a screenshot of the error log and contact Thales Customer Support.

Operational Issues

CCC maintains multiple log files that you can view to help troubleshoot operational issues you may encounter when using CCC. The logs are saved to:

Server Logs: **/usr/safenet/ccc/server/standalone/log/server.log**.

Monitoring Logs: **/usr/safenet/ccc/server/standalone/log/monitoring.log**

Operations Logs: **/usr/safenet/ccc/server/standalone/log/operations.log**

> **NOTE** We recommend that you delete any obsolete logs or move them to another location to reduce system clutter on the CCC server.

JDK Installation during CCC Server Configuration
If CCC is not successfully configured during JDK 1.8.0_171 version installation, the CCC administrator can perform the following steps:

1. Open the picketbox module.xml file:

vi /usr/safenet/ccc/server/modules/system/layers/base/org/picketbox/main/module.xml

2. Add the following dependency into the module.xml file:

<module name="sun.jdk"/>

3. Restart the CCC service.

Keystore Password Vault Error during CCC Server Configuration

If the keystore password fails to store in vault during CCC server configuration, then the CCC administrator can perform the following steps:

1. Open the picketbox module.xml file:

   vi /usr/safenet/ccc/server/modules/system/layers/base/org/picketbox/main/module.xml

2. Add the following dependency into the module.xml file:

   <module name="sun.jdk"/>

3. Re-run the following CCC server configuration script with old password or new password depending on the error message:

   sh config.sh

PED Connections

For devices with REST, if there is an active PED connection on the device that CCC is attempting to connect to (for example, if another session is executing "HSM login..."), the authorize request will wait until that action is done before continuing.

Root of Trust NTLS Connections

If you have connection problems with your Thales Luna Network HSM partition or root of trust, try examining the NTLS TCP keep alive setting. The root of trust terminates the NTLS connection if the connection is idle up to a set value of time, and unresponsive to a set number of transmissions. Follow the procedure to adjust these values. See the *LunaSH Command Reference* Guide for more information on the command, including acceptable ranges.

1. In LunaSH on your root of trust, run the following command to view the keep alive settings:

   lunash:> ntls tcp_keepalive show

2. Reset any values that you determine to be too small.

   lunash:>ntls tcp_keepalive set -idle <new_idle_time> **-interval** <new_interval_between_retries> **-probes** <new_number_of_retries>

3. Check that your settings were applied.

   lunash:> ntls tcp_keepalive show

4. Log into your CCC web server and open a terminal.

5. Restart the CCC service.

   systemctl restart ccc

Error Messages

Error message	Cause
Operation failed on host <hostname>. Crypto User activation failed. The operation requires the PIN to be initialized.	Attempt to authorize CU when CU not initialized
Operation failed on host <hostname>. Resource: https://<hostname>/api/lunasa/hsms/<HSM ID>/ partitions/<partition ID> was not found	Device becomes zeroized before initializing a service
Operation failed on host <hostname>. Error ID: LUNA_RET_SM_TOSM_DOES_NOT_VALIDATE	Device becomes zeroized before creating a service
The HSM at host <hostname> is zeriozed.	Attempt to authorize device that is zeroized
There was a problem connecting to <hostname>. Please check that the device is online and the host address and port number are correct.	Authorize device - HSM cannot be contacted (network service stopped)
Operation failed on host <hostname>. Error ID: LUNA_RET_HA_USER_NOT_INITIALIZED	Create service- click Finish while in the process of initializing HSM
Operation failed on host <hostname>. An error happened when attempting to connect to ped server.	Authorize device – PED server stopped
	Invalid PED server address
	Initialize Service – PED server stopped
	Initialize Service: PED server running but PED disconnected
Operation failed on host <hostname>. Error ID: LUNA_RET_CB_ABORTED	PED unplugged while initializing service
Operation failed on host <hostname>. Error ID: LUNA_RET_LICENSE_CAPACITY_EXCEEDED	Space remains on HSM, but no more licenses available (Add PPSO Service, Init PPSO service, Init Legacy Service)
Operation failed on host <hostname>. Error ID: LUNA_RET_HSM_STORAGE_FULL	Create Service - HSM out of space
A service with this name already exists. Please specify a unique name.	Create Service with name that already exists

Error message	Cause
Operation failed on host <hostname>. A duplicate item already exists	If service with same name was previously detached and you try to create a new one with that name
	Initialize Legacy Service – try to use a name that already exists
Operation failed on host <hostname>. Error ID: LUNA_RET_HA_USER_NOT_INITIALIZED.	Create service when HSM cannot be contacted (webserver service stopped)
Operation failed on host <hostname>. Resource: https://<hostname>/api/lunasa/hsms/<HSM ID>/partitions/<partition ID> was not found	Initialize Service when HSM cannot be contacted (webserver service stopped)
Operation failed on host <hostname>. Error ID: LUNA_RET_INVALID_CERTIFICATE_DATA	The user adds an HSM device whose webserver certificate is either not generated or is invalid.

Two Factor Authentication

If you have issues with using two factor authentication with CCC server, you can use the following procedure to reproduce the two factor authentication on CCC server:

1. Create an Application Owner or Administrator User in the **Accounts** section of the CCC server.
2. Select **Require two factor authentication** radio box.
3. Log out as the current user.
4. Log in to the CCC server as the two factor Application Owner or Administrator you have created.

   A **QR code** and a code string displays for authentication.
5. Enter the correct 6-digit OTP to go to the **new password** window.

> **NOTE** If CCC is still unable to validate the OTP, verify that the date / time and locale is properly synced with the server that is running CCC.

APPENDIX B:
Glossary

A

Administrator

The Administrator is the top level user of the CCC. The Administrator is able to add users and devices, create services, and perform server administration tasks on the CCC .

Application Owner

The Application Owner is an administrative role that can manage the services of an organization within the CCC. The Application Owner is able to deploy services for use by members of their organization.

C

certificate

A certificate is an electronic document used to prove and validate the ownership of a public key. If the key signature is valid, and the software examining the certificate trusts the issuers, then it can use that key to communicate securely with the certificate's subject.

certificate authority

A certificate authority is a trusted entity that issues digital certificates. This action certifies the ownership of a public key by the named subject of the certificate and allows for the establishment of a hierarchical trust between parties.

Crypto Officer

The Crypto Officer functions as the Partition Owner, in non-PPSO services. The Crypto Officer is responsible for initializing the Crypto User role, and for creating and modifying cryptographic objects in the HSM partition. The Crypto Officer is capable of key generation and deletion, key wrapping and unwrapping, content encryption and decryption, and key signing and verifying.

Crypto User

The Crypto User is an optional role that provides limited partition operations to a user. The Crypto User can access cryptographic materials on the partition for signing, verifying, encryption, and decryption, but cannot generate or delete keys or use them for wrapping objects.

D

device

Any hardware security module or appliance which is stored in the CCC application interface.

device pool

Devices can be organized into device pools. A device pool is a group of devices that are organized by purpose, version, owner, etc. Placing a device into a device pool has no effect on which users or organizations can access the device.

E

external database

An SQL database that is stored on an external server from the one the user has direct access to.

H

HA group

A High-Availability (HA) group consists of partitions organized for load balancing and redundancy across multiple HSMs. Partitions in the HA group are assigned active and standby states to ensure availability if a member HSM fails. The CCC allows users to manage and administer high-availability groups of Thales Luna HSM partitions.

High-availability configuration

A high-availability configuration is a method of active-active deployment of CCC application servers so that if one CCC application server goes down, another CCC application server can continue serving the requests

HSM

A hardware security module is a physical computing device that enables cryptographic services for a user. The CCC manages multiple HSMs.

K

keepalived

keepalived is a daemon load balancer used for configuring high-availability CCC servers.

keystore

A repository of security certificates (authorization certificates or asymmetric key sets) used for SSL encryption with the CCC.

L

load balancer

A device or software that acts as a reverse proxy and distributes network or application traffic accross a number of servers. A load balancer is used to increase the reliability of certain applications and systems. The daemon keepalived is an example of a load balancer.

local database

An embedded or SQL database that is stored on the same system as the CCC. It is accessed directly by the user.

M

monitoring

The monitoring feature provides access to data displays of managed device information. Monitoring allows users to instantly assess the status of all managed devices, and to access more detailed information for managed devices.

N

NTLS

A network trust link service uses two-way digital certificate authentication to protect sensitive data as it is transmitted between the HSM partition and client. Configuring NTLS between the CCC and a root-of-trust HSM device allows for secure data transfer over a trusted network.

O

organization

Organizations represent groups of Application Owners managed by the CCC. Application Owners are grouped into organizations where they can view and deploy the services created for and available to their organization.

OTP

A one-time password is used for the second stage of user verification during the two-factor authentication process. It is accessed through a two-factor authentication application on a personal mobile device.

P

partition

HSM partitions are independent logical HSMs that reside within the HSM appliance. Each HSM partition has its own data, access controls, security policies, and separate administration access independent from other HSM partitions. HSM partitions can be exclusive to a single client, or multiple clients can all share access to a single HSM partition.

PED

A PIN entry device is an electrically programmed key authentication device with a USB interface.

PPSO

Per-partition Security Officer (PPSO) is a security setting that, once enabled, requires each partition to have a unique Security Officer and password to enable crypto services.

private key

A private key is a string of code that is paired with a public key set of algorithms for text encryption and decryption. It is a component of public key cryptography used during asymmetric key encryption processes.

PSO

The Partition Ssecurity Officer (PSO) is responsible for initializing the Crypto Officer role on the partition, resetting passwords, backing up partition contents and setting and changing partition-level policies.

public key

A public key is a string of code that is paired with a private key set of algorithms for text encryption and decryption. It is a component of public key cryptography used during asymmetric key encryption processes.

R

reports

Reports provide detailed information about all managed devices and provisioned services on the CCC. Reports can be viewed, searched, and sorted in the CCC. They can then be printed or exported to a CSV file for external use.There are two primary types of reports generated by the CCC: service reports and device reports. The service report provides detailed information about each service managed by the CCC. The device report provides detailed information about the devices and associated partitions managed by the CCC.

root of trust

The root of trust is an HSM device that encrypts and decrypts all communications between the CCC and the connected HSMs. Setting up an HSM device as root of trust allows the CCC to log into the device as the HSM security officer using the root-of-trust HSM credentials.

S

script

An executable file designed to aid end users in configuring a program for operation on various systems and databases.

Security Officer

The Security Officer is responsible for the initialization of the HSM, setting and changing HSM policies, and the creation and deletion of application partitions.

service

A service refers to partitions on one or more HSM devices managed by the CCC. Services are assigned to, and owned by, specific organizations. Only members of the organization that owns the service are able to deploy and use the service for their cryptographic applications.

service template

To create a service the user must specify a template. Service templates specify the type, size, and capabilities of services created using the template. Service templates are reusable, allowing you to create templates for specific application types.

SSL

Secure sockets layer (SSL) connections allow the user to establish an encrypted link between any two systems. The connection is protected by an HSM device that encrypts and decrypts the data that passes over the connection.

STC

A secure trusted channel is a token-based secure channel between a Thales Luna HSM partition and its authorized users. It provides privacy of all communicated data, integrity assurance for all communicated data, and bi-directional authentication between HSM and client. This is a more secure method of data transfer than NTLS. An example of STC communication would be a connection between a client application server and an HSM partition.

T

two-factor authentication

Two-factor authentication increases security by enforcing dual-verification processes on CCC users. With two-factor authentication users are required to log in to the CCC using their administrative credentials and a time-based one-time password generated by an application on any secondary electronic device.