CCC 3.7

CUSTOMER RELEASE NOTES

Issue Date: 24 June 2021

Document Part Number: 007-012333-013 Rev. A

The most up-to-date version of this document is posted to the Customer Support Portal at https://supportportal.thalesgroup.com

Contents

Product Description

CCC is a web-based application that provides centralized management of your HSM infrastructure. With CCC, you can place some or all of your Thales Luna Network HSM devices into a common device repository, provision cryptographic services (HSM partitions) on these devices, monitor the status of your cryptographic devices and services, and then make these cryptographic services available to application owners on an organizational basis, for use with their cryptographic applications.

CCC provides an administrative interface and an application owner interface:

> the administrative interface is used by the organization responsible for managing your HSM infrastructure.

> the application owner interface is used by the consuming organizations to select and deploy the HSM resource available to them.

Release Description

CCC 3.7 rolls out several new features and enhancements aimed at saving the time and effort of the users, as well as eliminating known issues.

New Features and Enhancements

CCC 3.7 provides the following new features and enhancements:

External Directory Server Support over LDAP

The newly added directory over LDAP feature of CCC enables you to add, manage, and configure user directories over LDAP to provision users for CCC application. CCC has been tested with Microsoft Active Directory and RedHat Directory Server, and supports directory services over LDAP provided by various other vendors as well.

Device Log Export

You can use the device logs feature to:

> Export and download Managed Luna Network HSM logs.

> Export device logs to third party monitoring and analytics tools, such as Splunk.

Viewing Key Attributes

At the click of a button, you can now view the attributes of the keys present on the partitions associated with a service, including their Label, Type, Handle, Fingerprint, Algorithm, and Bit Size.

Improved Setup Process

The CCC installation and configuration process has been further automated.

ROT Self Activation

You can now allow CCC to cache your partition label and password by checking the **Remember Credentials** checkbox on the CCC Activation page to overcome frequent deactivation to Root of Trust due to network instability. When the CCC service shuts down, the cached root of trust label and password details get erased.

CentOS 8 and RHEL 8 Support

Support for CentOS 8 and RHEL 8 operating systems has been introduced in CCC 3.7.

SSL for DB Connection

Depending on your security requirements, you can now turn SSL for DB connection on or off during CCC configuration.

New Thales Branding

CCC UI has a new look and feel, in sync with the Thales brand.

Advisory Notes

This section highlights important issues you should be aware of before deploying this release.

Server Monitoring

We recommend monitoring your CCC server configuration with a server monitoring system. CCC cannot notify the users of a CCC instance deactivation in the event of a server outage or disconnection.

Thales Luna Network HSM 7.1 Monitoring HSM CPU Usage

The Thales Luna Network HSM 7.1 device firmware incorrectly reports the value for HSM CPU usage. The firmware will always populate the HSM CPU usage monitoring histogram value as 99.9%. This is not an accurate evaluation of the HSM devices performance by CCC.

Support for 5.x Devices

CCC 3.7 no longer officially supports 5.x devices. If you are managing primarily 5.x devices then you may desire to defer this software upgrade at this time. If you are managing a combination of 5.x and 6.x devices then the upgrade to CCC 3.7 will require upgrading your 5.x devices. See Managing Device Upgrades for more information about device upgrades.

Thales Luna HSM 7.1 and Newer Device REST API

On Thales Luna Network HSM 7.1 and newer devices, the REST API package comes pre-installed on the device. The user is still responsible for configuring the REST API on the device. It is recommended to use the latest REST API versions for better stability, as listed below.

- 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** NOTE: If STC is enabled, the webserver (REST API) of some Luna devices is required to be restarted.

ccc_client PED-Authenticated HSM Partition HA Group Service

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*.

Database Security

CCC supports tablespace encryption enabled through transparent data encryption (TDE) on an Oracle database. CCC does not currently support full disk encryption on a PostgreSQL database. As a result, the integrity of the database server is the responsibility of the user. We recommend keeping your database server in an environment that is secured by software data networks and firewalls. Customers are responsible for ensuring compliance with their organization's security policies.

Freemium License

The CCC Freemium virtual image is not available with the latest CCC 3.7 version. However, the Freemium license file is still supported with CCC 3.7 premium build. The Freemium license is available as part of the CCC software package.

> **NOTE** The CCC Administrator user can now use "Update License" button to replace the Freemium license file with the premium license when the product evaluation is completed.

Licenses

CCC versions 3.1 and newer are restricted by license. Users require a license file to make their instance of CCC operational. The license file defines the relative entitlements for CCC. A valid license file is required to access CCC as an Administrator or Application Owner and to enable the device/service monitoring feature. For more information about license types, consult the *CCC User Guide* or access Thales Customer Support Portal at https://supportportal.thalesgroup.com.

Mixed High Availability Device Partition Groups

7.x devices do not support mixed high availability (HA) device partition groups. You cannot create an HA partition group consisting of both 6.x and 7.x devices. HA partition groups can only consist of 6.x or 7.x device partitions.

Oracle Java JDK 8 Requirements

Previously released versions of Oracle Java JDK do not have a security.policy file. If you are using a previously released version of Oracle Java JDK you must download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 found at www.oracle.com. Three files are included with the download: a README and two jar files. To install the JCE Unlimited Strength Jurisdiction Policy, please refer to the README.TXT file provided in the zip package.

Java 1.8.0-144 JDK Memory Leak

The Java 1.8.0-144 JDK is not supported by CCC. The Java 1.8.0-144 JDK has a known security leak. It is recommended that you upgrade to the latest version of Java 1.8.0. For more information about the Java 1.8.0-144 JDK memory leak, review Java JDK issue 8164293.

Compatibility Information

For information regarding the supported hardware, software, and managed devices, consult CCC User Guide.

Feature Matrix for CCC 3.7

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 Material Visibility		6.x	6.10.9	7.1 or above
External Directory Server over LDAP		NA	NA	
Apply SW Package		7.3	N/A	7.x
Update Firmware		7.3	N/A	7.x

Upgrade Instructions

You can upgrade to CCC 3.7 from CCC 3.5, CCC 3.6, and CCC 3.6.1.

> **CAUTION!** CCC 3.7 is restricted by license. Ensure you have a license file available before upgrading to 3.7 or you will have restricted access to your CCC.

You must perform some configuration after upgrade to ensure access for existing managed devices and application owners.

Backing up Existing CCC Version

> **NOTE** The steps available here are for a PostgreSQL database. To back up an Oracle database, refer to the Oracle documentation which is available at the official Oracle website.

Take a full backup of all CCC files before you begin.

1. Enter the following commands to backup the existing Thales Crypto Command Center database:

   su - postgres

   pg_dump -f CCC_old_db_backup lunadirectordb

   The database is backed up to the following file:

   /var/lib/pgsql/CCC_old_db_backup

Upgrading CCC from the Existing Version

1. Go to the CCC installation directory:

   cd /usr/safenet/ccc

2. Launch the **uninstall.sh** script and respond to the prompts to uninstall. Retain your firewall port and database tables.

   sh uninstall.sh

   Do you really want to uninstall Crypto Command Center Server? [n]

   Do you want to close the port used by CCC in the firewall? [y]

   Do you want to drop database tables? [n]

   Do you want to remove all files in the support catalogue? [n]

   > **NOTE** If **y** is selected as the option, all the files in the support catalogue are deleted.

3. Install and Configure CCC 3.7, using the steps mentioned in the CCC User Guide.
4. Upload a License to CCC 3.7:
   a. The License Upload Modal displays.
   b. Click the **Upload License** button. The **Upload License** dialog displays.
   c. Click the **Upload** button and select the new license from your filesystem.

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

5. Distribute CCC Clients:
   a. From the Administration page, navigate to the Software Center to download an updated CCC client.
   b. Install this client on any application servers that access CCC.

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.

> **NOTE** Upgrading to 6.x may result in the loss of configured service templates, users, HA groups, and partitions on the HSM.

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 Network 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.

Known Issues

This section lists the issues known to exist in the product at the time of release. Workarounds are provided where available.

Issue Severity Definitions

The following table defines the severity of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Known Issues

Issue	Severity	Synopsis
CCC-8303	M	**Problem:** If you login with a newly created user, and stay on the "change password" screen for five minutes with no activity, when you then attempt a password change, you are redirected to a blank page. **Workaround:** This behavior indicates a timeout. You can reattempt login by clicking the back button, or by re-entering the Thales Crypto Command Center address into the URL bar in the browser.
CCC-8319	M	**Problem:** If you add a 6.x device, and then use LunaSH to alter the admin password and the REST API certificate, you cannot update either the admin password or the REST API certificate on Thales Crypto Command Center. If you add a 5.x device, and then use LunaSH to alter the admin password and the SSH host key, you cannot update either the admin password or the SSH host key on Thales Crypto Command Center. **Workaround:** Update Thales Crypto Command Center immediately after updating the admin password, SSH host key, or REST API certificate on the appliance. Do not perform any other configuration until Thales Crypto Command Center is updated. If you accidentally change both the device password and the device identity (SSH host key or REST API certificate) without updating Thales Crypto Command Center, use LunaSH to change the admin password back to the previous value. In Thales Crypto Command Center, verify the SSH key or REST API certificate. Then return to the device and change the admin password to the new desired password. Update the admin password in Thales Crypto Command Center.

Issue	Severity	Synopsis
CCC-8678	L	**Problem:** It is possible to create a service whose partition size is too small to store an STC client identity. If you attempt to authorize STC access to such a service through ccc_client, the operation fails. Each STC client registration uses 2332 bytes of storage on the partition. **Workaround:** If you intend to use STC with a new service, set the partition size to at least 5000 bytes to accommodate an STC client registration and still leave space for keys used in cryptographic operation. Consider partition storage needs when creating new service templates.
CCC-8819	M	**Problem:** If you create and deploy a service, change its organization, and then attempt to revoke access to the service, the full deregistration might not complete. For example, the revoke might not complete, the client entry might still be displayed in the service details tab, or the client might still be registered on the managed device partition(s). **Workaround:** If you attempted a revocation which did not complete, detach the service, re-import it, complete the normal application owner setup, and then revoke again. If you want to change a service's organization, first revoke client access, then change the organization, then deploy the service again. This ensures that future attempts to revoke access to the service will succeed.
CCC-9208	M	**Problem:** Monitoring data does not update automatically in the General and Capabilities tabs on the Device page. Monitoring information is retrieved and stored by the device, but is not generated automatically in the Thales Crypto Command Center graphic user interface on the General tab and the Capabilities tab. **Workaround:** Click Refresh in the Capabilities tab to generate up-to-date monitoring data.
CCC-10174	L	**Problem:** When sorting a Service Report, at times the Sort drop down menu loses its interface layer priority, appearing behind the entries in the Services List. **Workaround:** Minimize and expand the row where the issue is occurring.
CCC-11976	M	**Problem:** STC partition can not be created through CCC. Workaround: Use LunaCM if STC partition is required.
CCC-12638	M	**Problem:** Sometimes due to network latency, ccc_client.jar fails to authorize the services on Windows machine. **Workaround:** Check the network latency and retry. If the issue continues, use ccc_client.jar based on Linux machine.
CCC-12639	M	**Problem:** If the ccc_client.jar is run without trusting the server certificate, it throws an exception when Option 4 (exit) is directly selected after the run. **Workaround:** Always trust the server certificate when the ccc_client.jar is run.
CCC-13073	L	**Problem:** Status of a imported user does not change in CCC even when state is changed in external directory server. **Workaround:** Manually delete the user and then import again.

Issue	Severity	Synopsis
CCC-13259	M	**Problem:** Sometimes when NFS server goes down in CCC High Availability setup, NFS clients becomes unresponsive. **Workaround:** Re-run `enableNFSSharing.sh` script on client side for NFS connection.
CCC-13260	M	**Problem:** Sometimes when a new NFS client is added to an existing High Availability CCC setup, permissions on shared folder of existing NFS clients change to some unknown permission. **Workaround:** Change the permission on shared folder /usr/safenet/ccc/packages and /usr/safenet/ccc/lunalogs to lunadirector.
CCC-13364	H	**Problem:** When HA service is created with whitespace in its name, then HA authorization using ccc_client and NTLS creation in key material visibility fails. **Workaround:** Avoid using whitespace in HA service name. **NOTE** This issue will be fixed in a forthcoming CCC patch release.

Supported Versions of CCC

The supported versions of CCC are:

> CCC 3.7

> CCC 3.6.1

> CCC 3.6

> CCC 3.5

The latest End of Sale (EoS) version information can be found on the link given below:

https://supportportal.gemalto.com/csm?id=kb_article_view&sys_kb_id=6cfb01b91ba5485cf2888739cd4bcb68&sysparm_article=KB0020550

> **NOTE** The CCC users are recommended to upgrade to the latest CCC version. The list of supported versions can be found at the Customer Support Portal, at https://supportportal.thalesgroup.com.

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.