# CipherTrust Cloud Key Manager

## Patch Notes

- **Patch Release 1.7.1, Version: 1.7.1.29740**
- **Date: June 30, 2020**

### New Features and Enhancements

There are no new features in this release of CipherTrust Cloud Key Manager (CCKM). This release provides the following new enhancement:

**Security Enhancement**
CCKM 1.7.1 addresses a cross-site-scripting (XSS) vulnerability. You are advised to upgrade to this patch release of CCKM to resolve this XSS issue.

### Restrictions

The following restrictions apply to this release of CCKM:

- DSM domain name must not exceed 22 characters.
- KeySecure supports all cloud services that CCKM supports with the exception of Azure Stack.
- Only local users are supported on KeySecure version 1.8.0. This is not a restriction on the newer version of KeySecure. On KeySecure version 1.9.1.4281, local and LDAP users are supported.

# Upgrade to CCKM 1.7.1

In this release, upgrading to CCKM is supported through the use of the upgrade CLI command.

## Prerequisites

The following are the prerequisites steps to take prior to upgrading CCKM:

- Initialize the MongoDB database holding the 1.7.0 CCKM data.
- Configure an HTTPS-based file server with an SSL certificate. It is recommended you configure an SSL certificate that is signed by an external Certificate Authority (CA) for the file server. You can also configure the file server to use a self-signed certificate. However, upload the root CA certificate to CCKM using following CLI command:

```
system> security --addcert <alias>
```

- Upload the upgrade tar file to an HTTPS-based file server.
- Backup the database, key source, and CCKM instance. An upgrade from 1.7.0 to 1.7.1 does not support a "restore" operation. CCKM does not provide a way to backup the entire CCKM solution instance. Hence it is **mandatory** to perform these backups before initiating an upgrade. The backups should be taken by infrastructure supported ways. For example, take snapshots of the VMware ESX deployment, AWS, or Azure VM backups (depending on the deployment method you are using).

## Upgrade from CCKM 1.7.0 to 1.7.1 using CLI

NOTE: If you have a CCKM cluster, you are required to perform the upgrade on each CCKM instance within the cluster.

NOTE: ***Before*** **performing an in-place upgrade for a CCKM instance, be sure to backup your MongoDB, Key Source and CCKM instance. CCKM should be inactive when this backup is performed to avoid data corruption.**

NOTE: *Appendix A: CCKM CLI Commands* in the *CipherTrust Cloud Key Manager Installation & Configuration Guide 1.7.1* provides a high-level overview of each of the CCKM command categories that are available. For information about the details of each command and its options, run the command with the "--help" option within the CCKM CLI. Refer to the "*CCKM CLI Navigation*" section within this appendix for more information.

To upgrade your existing CCKM version 1.7.0 to 1.7.1, do following:

1. From Thales Support site, download the following file:
   `UPGRADE_1.7.1_3879f4be_ca1dc682_29740.tar.gz`

2. Upload the file to an HTTPS web site, and note the URL. For example, if you upload the file to AWS S3, an example URL is:

   *https://s3.amazonaws.com/cckm/UPGRADE_1.7.1_3879f4be_ca1dc682_29740.tar.gz*

   **Note**: Ensure the tar file is publicly accessible on the site.

3. As a CCKM CLI administrator, log on to the 1.7.0 CCKM CLI.
4. In the CCKM CLI prompt, enter the **maintenance** command category and then enter the **upgrade** command replacing "<upgrade package url>" with the noted HTTPS web site:

```
maintenance> upgrade <upgrade package url>
Usage: upgrade <upgrade package url>
maintenance> upgrade https://s3.amazonaws.com/cckm/cckm1.7.1.tar.gz
WARNING: Please backup your current database and CCKM virtual
machine.
If you don't have backup then you must not continue with this upgrade
process.
Do you wish to continue? <y/n> [n]:
```

5. Enter **y** to proceed with the upgrade.
   After a successful upgrade, the CCKM instance reboots automatically.

## Restore to Previous CCKM

If the upgrade fails, restore the CCKM instance, key source and database that you backed up before starting the upgrade.

## Troubleshooting

### SSL Verification Fails

If SSL verification fails during the upgrade process, you will receive an error message in the CCKM CLI such as the following:

```
Error:
maintenance> upgrade https://s3.amazonaws.com/cckm/cckm1.7.1.tar.gz
WARNING: Please backup your current database and CCKM virtual
machine.
If you don't have backup then you must not continue with this upgrade
process.
Do you wish to continue? <y/n> [n]:
Fetching the tar...https://s3.amazonaws.com/cckm/cckm1.7.1.tar.gz
ERROR: Unable to download
https://s3.amazonaws.com/cckm/cckm1.7.1.tar.gz
ERROR: SSL verification failed.
```

### Solution

Ensure you have uploaded the root CA certificate of the HTTPS file server to the CCKM server. Otherwise, you will receive the above error message.

To upload the root CA certificate of the HTTPS file server to the CCKM server, do the following:

1. Access the CCKM **system** command category:

```
cckm> system
```

2. Access the security settings and upload the root CA certificate to the CCKM server:

```
system> security --addcert <root CA certificate alias>
```

If you are working with the Thales support team on troubleshooting this issue or plan to contact them about this issue, first collect the CCKM debug logs to send to them. There are two methods in which to collect these logs. One method is by clicking on **Download Debug Logs** on the **Logs** page within the CCKM Admin Portal. The other method is by using the **upload** command within the **applog** command category of the CCKM CLI.

To collect the CCKM debug logs using the CCKM CLI, do the following:

1. Access the CCKM **applog** command category and upload the logs to a destination host (such as your laptop or desktop) specifying your username and the directory path to which to save these logs:

```
applog> upload --host example.com --user example_user --path
/example/data
```

```
usage: upload [-h] [--host DESTINATION_HOST] [--user USER] [--path
DIRECTORY]

CCKM logging operations
options:
```

```
  -h, --help            show this help message and exit
--host DESTINATION_HOST
                      Destination host to which application logs are to
be copied.
--user USER           Username of destination host
--path DIRECTORY      Destination directory
```

2. Send the CCKM logs to Thales support.

## Synchronize CCKM Local time with Network Time using NTP Server

In this release of CCKM, the local time on CCKM server is no longer synchronized with the network time. ***After installing*** CCKM and changing the default password, the ***first*** step to take is to synchronize the local time with network time using your preferred Network Time Protocol (NTP) server(s). For example purposes, the “pool.ntp.org” is used as the NTP server. However, you can use any NTP server you wish to use.

NOTE: At least one NTP server must be configured ***before*** you configure to add the NTP server to CCKM and synchronize with it.

To add an NTP server to CCKM and synchronize the CCKM local time to the network time, do the following:

1. Access your CCKM server through SSH (such as Putty):

```
ssh cliadmin@<cckmhost>
```

2. Enter your user password when prompted:

```
cliadmin@>cckmhost>'s password:
CCKM CLI Main Menu
cckm>
```

3. Access the CCKM Network command category:

```
cckm> network
```

4. Access the NTP service settings and add the named NTP server to contact for time synchronization:

```
network> ntpservice --add pool.ntp.org
NTP Servers:
   pool.ntp.org
```

5. Perform immediate clock synchronization with the configured NTP server:

```
network> ntpservice --sync
Synchronizing time with NTP server(s):
   pool.ntp.org

   19 Mar 23:23:25 ntpdate[18641]: step time server 217.91.44.17 offset
29286.555701 sec
```

6. Verify that the status of the NTP service is enabled:

```
network> ntpservice --status
enabled
Active: active (running) since Thu 2020-03-19 14:58:26 PDT; 8h ago
No association ID's returned
network>
```

## CCKM and DSM Compatibility Matrix

Table 1 shows the compatibility between the CCKM and DSM software versions.

Table 1: CCKM and DSM Software Compatibility Matrix

| CCKM SW Version | DSM SW Version | | | | | |
|---|---|---|---|---|---|---|
| | 6.1.0.9118 | 6.2.0.12051 | 6.3.0.13038 | 6.4.0.15031 | 6.4.1.15556 | 6.4.2.16023 |
| 1.6.0.6198 | Compatible | Not Compatible | Not Compatible | Not Compatible | Not Compatible | Not Compatible |
| 1.6.1.6542 | Compatible | Compatible | Not Compatible | Not Compatible | Not Compatible | Not Compatible |
| 1.6.2.16370 | Compatible | Compatible | Compatible | Not Compatible | Not Compatible | Not Compatible |
| 1.6.3.20532 | Compatible | Compatible | Compatible | Compatible | Not Compatible | Not Compatible |
| 1.7.0.26046 | Not Compatible | Not Compatible | Not Compatible | Compatible | Compatible | Compatible |
| 1.7.1.29740 | Not Compatible | Not Compatible | Not Compatible | Compatible | Compatible | Compatible |

## CCKM and KeySecure Compatibility Matrix

Table 2 shows the compatibility between the CCKM and KeySecure software versions.

Table 2: CCKM and KeySecure Software Compatibility Matrix

| CCKM SW Version | KeySecure SW Version | | |
|---|---|---|---|
| | 1.8.0.3506 | 1.9.1.4281 | 1.10.0.4610 |
| 1.6.3.20532 | Compatible | Compatible | Compatible |
| 1.7.0.26046 | Compatible | Compatible | Compatible |
| 1.7.1.29740 | Compatible | Compatible | Compatible |

CCKM supports the KeySecure types of K570, K170 Luna SA7 (Network Luna HSM), and K170.

## CCKM and MongoDB Migration Path

Table 3 shows the supported migration paths of MongoDB on CCKM version 1.7.0 to MongoDB on CCKM version 1.7.1:

- **(Row 1)** Existing MongoDB instance(s) *without* SSL/TLS on CCKM version 1.7.0 to migrate to existing MongoDB instance(s) *with* SSL/TLS on CCKM version 1.7.1, and then finally to MongoDB Atlas on CCKM version 1.7.1.
- **(Row 2)** Existing MongoDB instance(s) *without* SSL/TLS on CCKM version 1.7.0 to migrate to MongoDB Atlas on CCKM version 1.7.1.
- **(Row 3)** Existing MongoDB instance(s) *without* SSL/TLS on CCKM version 1.7.0 to migrate to existing MongoDB instance(s) *without* SSL/TLS on CCKM version 1.7.1. From this, migrate to existing MongoDB instance(s) *with* SSL/TLS on CCKM version 1.7.1 and then finally to MongoDB Atlas on CCKM version 1.7.1.
- **(Row 4)** Fresh install of MongoDB instance(s) *with* SSL/TLS on CCKM version 1.7.1 to migrate to MongoDB Atlas on CCKM version 1.7.1.
- **(Row 5)** Fresh install of MongoDB instance(s) *without* SSL/TLS on CCKM version 1.7.1 to migrate to MongoDB instance(s) *with* SSL/TLS on CCKM version 1.7.1. From this, migrate to MongoDB Atlas on CCKM version 1.7.1.
- **(Row 6)** Existing MongoDB Atlas on CCKM version 1.7.0 to migrate to MongoDB Atlas on CCKM version 1.7.1.

Table 3: CCKM and MongoDB Software Migration Matrix

| Row | CCKM 1.7.0 | CCKM 1.7.1 | CCKM 1.7.1 | CCKM 1.7.1 |
|---|---|---|---|---|
| 1 | MongoDB without SSL/TLS | MongoDB with SSL/TLS | MongoDB Atlas | N/A |
| 2 | MongoDB without SSL/TLS | MongoDB Atlas | N/A | N/A |
| 3 | MongoDB without SSL/TLS | MongoDB without SSL/TLS | MongoDB with SSL/TLS | MongoDB Atlas |
| 4 | N/A | Fresh install of MongoDB with SSL/TLS | MongoDB Atlas | N/A |
| 5 | N/A | Fresh install of MongoDB without SSL/TLS | MongoDB with SSL/TLS | MongoDB Atlas |
| 6 | MongoDB Atlas | MongoDB Atlas | N/A | N/A |

## Resolved Issues

| Issues | Summary | Description |
|---|---|---|
| CT-3303 | Kmaas service automatically restarts after every 1 min | After uploading a license to CCKM, which expires within 90 days, the kmaas service repeatedly restarts after a minute. |
| CT-3339 | IBM upload key - Unable to create import token | Uploading any root key from the IBM **Keys** page within the CCKM user portal to IBM Key Protect fails. |
| CT-3348 | IBM - Key rotation policy first change in IBM is not synchronized | If you create a rotation policy for a key in the IBM Key Protect portal, and then proceed to manually synchronize the key in CCKM, the rotation policy is not synchronized although a success message displays. From the **Update Key** dialog box (accessed from the IBM **Keys** page), the **Enable auto-rotation in key policy** toggle is set to **Off** for the given key**.** The expected behavior is for the toggle to be set to **On** indicating the key synchronization was successful. |

## Known Issues

| Issues | Summary | Description | Workaround Solutions |
|---|---|---|---|
| CT-1013 | Azure service principal - Shows a blank page after admin consent is done using IE 11 browser | When you log into CCKM for Azure using CCKM as a service principal for the first time, you are required to provide your admin consent to grant permissions to the CCKM app to access your Azure resources. However, when you use the Internet Explorer (IE) 11 browser to provide your admin consent, you encounter an issue. After you click the **Admin consent** button from the **CCKM Admin Consent** dialog box to submit your consent, and you are redirected to the Microsoft login page to login, a blank page displays after the login. Instead, the Azure CCKM dashboard should display after a successful login. | This issue is not encountered when using either Chrome or Firefox. Use these browsers instead of IE 11 when logging into CCKM for Azure. |

| Issues | Summary | Description | Workaround Solutions |
|---|---|---|---|
| CT-1574 (or GATEWAY-4082) | IE browser - sort icons in Keys page does not show after refreshing the browser | If you use the IE 11 browser, and you refresh the browser, the sort icons in the table column headers disappear. You can still sort columns by clicking the column header. | There is no workaround to show "sort icon" on IE. The only workaround is to use different browser. |
| CT-1575 (or GATEWAY-3179) | If you have set up Azure AD Conditional Access and thereafter your access is blocked by the Azure conditional access policy, you may encounter an Internal Server Error | N/A | If you encounter this issue, refresh the page, click the browser back button or open the page in a new tab. |
| CT-2238 | Using IE browser, icons in the left navigation bar of the Admin portal do not display. | Using the IE 11 browser, text instead of icons displays in the left navigation bar of the Admin portal for each of the available pages. | Use a different browser to view the icons. |
| CT-2807 | New admin portal - throws error message after trying few times entering wrong DSM details | When you enter an incorrect DSM IP address multiple times in the CCKM admin portal > **Key Sources** page > **DSM Configuration page**, CCKM throws an error message indicating it cannot connect to the DSM. After entering the correct IP address and clicking the **Save** button, the same error message displays again. | Click on the **Save** button again, and the error message will no longer display. The data is saved successfully. |
| CT-2850 | New admin portal - **Logs** page heading UI issue | In the **Logs** page, the table column heading is not aligned with the rest of the table. | None |
| CT-3021 | Display problem on IE11 browser on AWS Cloud schedule page | When more than one schedule is configured on the **Schedules** page within the CCKM user portal for the AWS cloud, the **Actions** list for the second configured schedule is hidden when using IE11. | On IE11, scroll down the **Actions** list to view the second schedule. This issue is not encountered on Chrome and Firefox. |
| CT-3064 | **Save** and **Cancel** buttons are not click-able in the Chrome and Firefox browsers when adding cloud accounts and subscriptions on **Licenses** page | When using the Chrome and Firefox browsers, the entire **Save** and **Cancel** buttons are not click-able when adding cloud accounts and subscriptions on the **Licenses** page within the CCKM admin portal. | Hover around the text box to find the click-able part of **Save** and **Cancel** buttons on top left corner. |

| Issues | Summary | Description | Workaround Solutions |
|---|---|---|---|
| CT-3075 | Using IE11 on admin portal, upload wrong DSM certificate first and then upload correct one will continue getting error message. | Once an invalid DSM certificate is uploaded as part of the DSM configuration in the **DSM** tab within the **Key Sources** page of the admin portal, the same error displays even after uploading a valid DSM certificate. | Log out of the admin portal, log in again, and then proceed with the DSM configuration. The error message will no longer display after uploading a valid DSM certificate. |
| CT-3076 | Cannot set AWS schedules through CCKM REST API when using temporary credentials | For users who are authenticating to CCKM REST API using AWS temporary credentials, an error message displays when configuring schedules. | Set up your schedules outside of CCKM. |
| CT-3077 | When adding a new user within admin portal, the **Submit** button is disabled even when all the required fields are filled | After entering all of the *required* information marked with "*" in the **User** dialog box (in the CCKM admin portal > **Settings** page > **User Management** tab) to add a new user, the **Submit** button remains disabled. | Enter information in *every* field in the **User** dialog box. Thereafter, the **Submit** button is enabled. |
| CT-3097 | CCKM does not failover to the second DSM node in the cluster, if the primary DSM fails | When CCKM is configured with a DSM cluster setup with High Availability (HA) and the primary DSM fails, CCKM does not connect to the second DSM node. | ***Prior*** to configuring DSM as the key source in CCKM, use the DSM CLI to update the host file (`/etc/host`) of each DSM appliance in the cluster with the hostname and IP address of the given DSM. |
| CT-3148 | Admin portal errors on Monitor page | On the **Health Monitor** page within the CCKM admin portal, the GUI displays a DSM connection error message twice when the DSM is down. | None |
| CT-3195 | CCKM cluster node does not update the IP and certificate of DSM/KeySecure | When an IP address and/or a certificate of a DSM or KeySecure on **Key Sources** page is updated for one CCKM in a CCKM cluster, this information does not get propagated to the second CCKM. | Manually update the IP address and/or certificate configuration of the DSM or KeySecure (depending on the key source you are using) from the **Key Sources** page on all the CCKM nodes in the cluster. |

| Issues | Summary | Description | Workaround Solutions |
|---|---|---|---|
| CT-3825 | A decimal number, such as 2.5, can be entered for the value of the key rotation interval in the **Update Key** dialog box. | When updating a key from the **IBM Keys** page, entering a decimal number for the key rotation interval in the **Update Key** dialog box is permitted. However, only integers from 1 to 12 are permitted indicating the number of months for the interval. | Enter an integer from 1 to 12 for the key rotation interval. |
| CT-3827 | Advanced search on the **IBM Keys** page does not return results if **Rotation Status** is set to filter on *both* "Auto Rotate On" and "Auto Rotate Off". | If you select to filter on *both* "Auto Rotate On" and "Auto Rotate Off" for **Rotation Status** when running an advanced search within the **IBM Keys** page of the IBM user portal, a status message displays indicating the page is loading. The page then hangs, and no search results are returned. | Do not select "Auto Rotate On" and "Auto Rotate Off" at the same time. |
| CT-3847 | None of the available actions display in **Actions** column after initial automatic synchronization starts and then completes while on the **Keys** page. | If you go to the **Keys** page of the IBM user portal after the initial automatic synchronization starts and then completes, none of the available actions for the keys display within the **Actions** column. | Navigate to another page within the user portal and then go back to the **Keys** page. The available actions for the keys display. |
| CT-3852 | Results of IBM Combined Key Activity Reconciliation Report and IBM Key Activity Report do not match IBM LogDNA report. | For the same key operations, the IBM Combined Key Activity Reconciliation Report and IBM Key Activity Report provide less information than the IBM LogDNA report. | None |
| CT-3870 | Last rotation date of an IBM root key is not updated after it is enabled for autorotation and successfully auto rotated. | Last rotation date of an IBM root key is not updated in the **Key Details** page after it is enabled for autorotation and successfully auto rotated. This issue occurs intermittently. | Manually synchronize your IBM keys in CCKM to view the correct date for the last rotation. |

## Sales and Support

For support and troubleshooting issues:

- https://supportportal.thalesgroup.com
- (800) 545-6608

For Thales Sales:

- https://enterprise-encryption.vormetric.com/contact-sales.html
- sales@thalesgroup.com
- (888) 267-3732

# Notices and License

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

**Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.**

**Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.**