CipherTrust Manager k160
Quick Start Guide

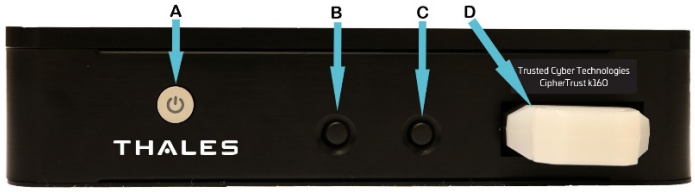
This document details quick instructions for starting up and configuring a Thales Trusted Cyber Technologies (TCT) CipherTrust Manager k160 appliance. Full documentation is located here: https://www.thalesdocs.com/ctp/cm/latest/get_started/deployment/index.html.

Required Equipment

- Power supply and cable
- Serial-to-USB adapter cable
- Null Modem cable
- (2) Mounting brackets with screws
- CipherTrust Manager k160 Appliance
- (2) USB HSM Tokens (Standard or High Assurance)
- USB Extender Cable (High Assurance only)
- Ethernet cable (not included)

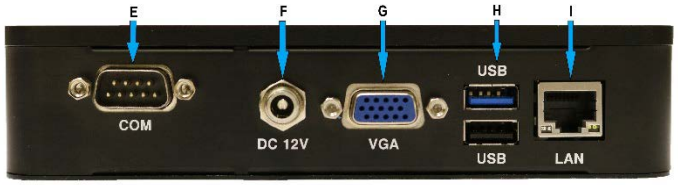
WARNING: To avoid inadvertently locking the USB token HSM, wait to insert the first USB token HSM until ready to proceed with the "*Perform the Initial Token HSM Setup"* instructions below. Also, **tokens are specific to a particular k160 and are not interchangeable.**

Front of Unit



Item	Name	Description
A	Power On/Off	Powers the appliance on or off.
B	Zeroization Button 1	Resets the k160. Both buttons must be pressed for 5 seconds. Disabled by default.
C	Zeroization Button 2	Resets the k160. Both buttons must be pressed for 5 seconds. Disabled by default.
D	USB Token HSM	Standard or High Assurance. (High Assurance token shown.)

Back of Unit



Item	Name	Description
E	(COM) Console Port	Connect a terminal to this port using the included DB9 to USB cable.
F	DC 12V	Power Adaptor connection.
G	VGA	Connect a standard VGA monitor.
H	USB ports	Used to register additional tokens.
I	LAN	CAT5 Networking Port.

Physical Installation

1. Install the CipherTrust k160 in an appropriate mounting rack that provides sufficient space front, side, and back for cabling, airflow, and maintenance.
2. Connect the provided Null Modem cable to the COM port (E). If your computer does not have a serial port, use the provided Serial-to-USB adapter cable.

   NOTE: If the adapter is not recognized by your computer, you may need to install a USB driver. Contact TCT Technical Support for assistance.
3. Insert an Ethernet cable into the LAN port (I) and connect the other end to the network.
4. Insert the power cable into the DC 12V (F) and then plug to an AC power source. The CipherTrust k160 will power up automatically.
5. Press the power button (A) to turn off.

Establish a Connection and Change Default Passwords

Open a Serial Connection

A serial connection is initially required to set administrative credentials and perform any necessary network configurations.

1. Connect the Null Modem cable to the COM port on the back panel of the k160. If your computer does not have a serial port, connect the Serial-to-USB adapter cable between the Null Modem cable and a USB port on your computer.

   NOTE: If your system does not automatically install the USB driver, contact TCT Technical Support for assistance.

2. Use a terminal emulation package, such as PuTTY, to open a serial connection to the k160. Set the serial connection parameters as follows:

   VT100/ANSI
   Baud rate: 19200
   Data bits: 8
   Parity: None
   Flow Control: None
   Stop bits: 1

   NOTE: You may need to press ENTER several times to start the session.

3. When the connection is made, a DHCP-assigned IP address appears together with the appliance login prompt:

   ```
   ciphertrust login:
   ```

4. As the System Administrator, enter "**ksadmin**" to log in and follow the prompts to create a secure password.

   The system services start to launch at this point, which can take several minutes.

5. To set a static IP address, use NMCLI:

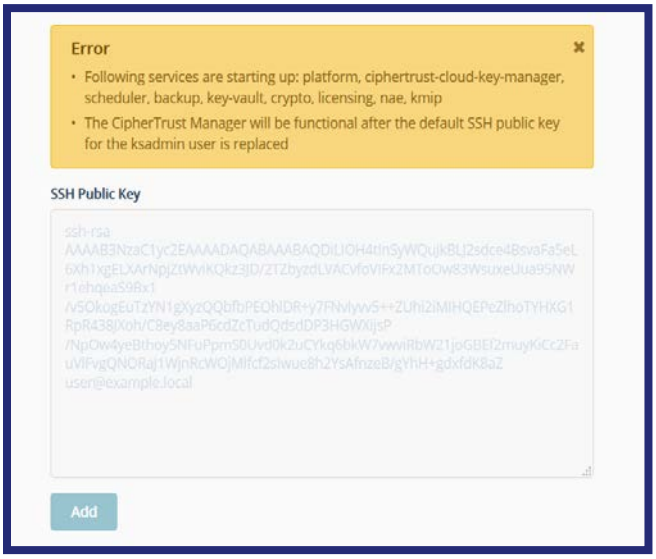
   ```
   nmcli conn modify "Wired connection 1"
   ipv4.method manual ipv4.addr <k160 IP/netmask
   (CIDR)> ipv4.gateway <Gateway IP> ipv4.dns
   <comma separated IPs>

   nmcli general hostname <hostname.domain>

   nmcli conn up "Wired connection 1"

   nmcli conn show "Wired connection 1"
   ```

   NOTE: See, "CipherTrust Manager > Getting Started > CipherTrust Manager Deployment > Network Configuration Tutorial" in the full product documentation.

6. [Optional] Close the serial connection.

Connecting to the GUI for the first time

1. In a web browser, navigate to the IP address displayed or set via the serial connection. The error displayed is normal.



2. Paste into the field your SSH Public Key and then select **Add**.

   NOTE: The SSH Public Key must be a 'PEM-formatted RSA key'. You can generate this key using 'PuTTYgen' or similar utility.

   WARNING: Be sure to store and securely protect the associated private SSH key, as this key will be required to SSH to the appliance.

3. Log in using the initial default credentials:

   Username: admin
   Password: admin

4. Enter a new password using this default Password Policy:

   Length: 8-30 characters
   At least 1 each: uppercase, lowercase, digit, and other

   Log in again using this new password. The CipherTrust Manager Web Page appears.

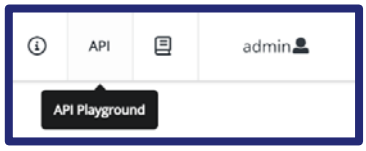
Root of Trust Configuration

The CipherTrust k160 utilizes a token HSM as its root of trust. After registering the first token HSM, additional tokens may be added.

NOTE: Each token is labeled with a small white label indicating the unique lock code corresponding to a particular k160. A similar white label is found on the right front of the k160. Ensure the tokens match correctly with the k160 unit, and further label them as either primary or backup HSM tokens once configuration is completed.

Download the CLI Toolkit

1. In the web GUI, click the "API" button at the far right of the top title bar to open the API Playground.



2. On the top left, click into the CLI Guide.

3. Click on the blue CLI button at the top right to download the **ksctl_images.zip** package.

This package contains the CLI tools and sample configuration file to initialize the HSM tokens to the k160.

NOTE: Download a fresh copy of the ksctl_images.zip from the k160 that is being deployed as previous versions may not be compatible.

4. Unpack the ZIP archive on your client workstation.

5. Navigate to the **ksctl_images** directory, copy the **config_example.yaml** under a new name (e.g. "k160.yaml"), and modify these lines within:

```
KSCTL_URL: <k160 IP>:443
KSCTL_PASSWORD: <password set in GUI above>
KSCTL_TIMEOUT: 360
```

Perform the Initial Token HSM Setup

1. **Insert the first token HSM** into the front slot of the k160.

   NOTE: Verify that the tokens are firmly inserted into their USB interfaces and, if applicable, the High Assurance token is NOT illuminated red.

2. From the CLI toolkit (**ksctl_images**) directory, execute the following command specifying the "k160.yaml" file created in step 5 from *HSM Root of Trust Configuration* above:

```
ksctl --configfile "<path>\<k160>.yaml" hsm setup k160 --reset [--ha | --std]
```

   "--ha" for High Assurance **|** "**--std**" for Standard

   The HSM configuration validates and the system will reset.

   NOTE: If you attempt to log in on the GUI, you will see various messages about services starting up and it may take over 10 minutes to complete the start-up process.

3. Refresh the browser window, accept the new certificate and proceed to the IP address of the k160. Log back into the GUI with the **original login credentials** (admin/admin) and reestablish a new admin password.

4. Verify the HSM token has been set up by visiting the "Admin Settings ➔ Root of Trust" page.

Register an Additional Token HSM

1. **Keeping the first token inserted into the k160**, insert another token into a USB slot on the back of the k160. For HA models, use the provided USB extender cable.

2. From the CLI toolkit (**ksctl_images**) directory, execute the following command to turn on Maintenance Mode:

```
ksctl --configfile "<path>\<k160>.yaml" hsm tokens maintenance set --maintenance-on
```

   This will prevent some of the services from starting which will allow for registration of the additional token.

3. Issue this command to register the additional token HSM:

```
ksctl --configfile "<path>\<k160>.yaml" hsm tokens reg
```

4. Once the command completes, **remove the additional token from the back of the k160**.

5. Turn off Maintenance Mode:

```
ksctl --configfile "<path>\<k160>.yaml" hsm tokens maintenance set --maintenance-off
```

   WARNING: Do not operate the k160 with both HSM tokens inserted. Be sure to test operation using either token.

Enabling the Zeroization Buttons

The Zeroization Buttons (B & C) on the front of the k160 may be enabled to provide quick reset capabilities via the **kscfg** utility (as *ksadmin* via SSH or console):

```
kscfg k160 buttons disable|enable|status
```

- disable: disables k160 buttons functionality
- enable: enables k160 button functionality
- status: shows k160 button functionality status

Output of the **kscfg k160 buttons status** command:

```
$ kscfg k160 buttons status
{
        "Enabled": true
}
```

Operating the Zeroization Buttons

The Zeroization Buttons are activated by simultaneously depressing and holding down both buttons for 5 seconds.
Once activated, the k160 CipherTrust Manager:

1. wipes the token of all objects (if token HSM is present);
2. clears the SSH key;
3. removes any custom networking configuration;
4. removes the CM log files, akeyless log files and audit log files;
5. removes system backups and backup keys
6. removes/resets the "ksadmin" password (must be reset at next login);
7. removes upgrade files and upgrade logs;
8. performs a system reset (similar to **kscfg system reset** command);
9. powers off the device after approximately one minute.

NOTE: The LED light on the power button (A) will turn off with the system shutdown to indicate success of the operation.

After this has completed, all token HSMs will need to be reset and re-registered (See "*Performing the Initial Token HSM Setup*").

NOTE: Support for the physical zeroize buttons requires minimum CM v2.15.0. In versions prior to CM v2.21.0, activating the zeroization buttons deletes the Root of Trust keys on any connected token HSM and performs a system reset to wipe all locally stored data – no additional items are reset.

Removing a Token During Operation

Removing the token HSM triggers the system services to shut down within 1 minute, shutting off all access to cryptographic materials and rendering keys, stored objects, etc., encrypted and unusable.

- The system services enter into a restart loop, checking for the reintroduction of a registered token HSM.
- Once a registered token HSM is provided, the system will start back up and resume operations.
- Stored objects are recovered by reintroducing a registered token HSM or by performing a system reset and restoring from a backup.

Troubleshooting

Issue	Resolution
HA Token HSM lights up red after being inserted for a period of time	The HA Token HSM has locked itself and needs to be power cycled. Remove the token HSM from the appliance, wait ~10 seconds, and then reinsert into the USB slot. If performing initial configuration, wait to insert the HA Token HSM until ready to proceed with the "*Perform the HSM Setup*."
HA Token HSM lights up red immediately after being inserted.	Contact Thales TCT Technical Support.