

u.trust Anchor LAN V5 FIPS 140-3

Quick Start Guide



utimaco[®]

Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet e-mail	https://support.hsm.utimaco.com/ support@utimaco.com

Document Version	Working Version; 1.0.2
Product Version	6.0.0
Date	2024-10-22
Document No.	
Status	2024-0016

PUBLISHED

All rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>
---------------------	--

Table of Contents

1	Introduction	4
1.1	Security Guidelines.....	4
1.1.1	General Advice.....	4
1.1.2	Protected Operational Environment	5
1.1.3	Protection of Data Outside the u.trust Anchor	6
2	Overview	8
2.1	Architecture.....	10
2.2	Templates.....	12
2.3	u.trust Anchor Product Line	13
3	Getting Started	16
3.1	Switch on the u.trust Anchor LAN	16
3.2	Configure the IP Address (e.g., static IPv4).....	17
3.3	Configure the IP Address for the Default Gateway	18
3.4	Enable the SSH Daemon.....	19
3.5	Preparation Steps on the Administration Computer.....	20
3.5.1	Install Java	20
3.5.2	Install gladm	20
3.5.3	Install csadm	22
3.5.4	Log in Remotely and Change the Default Password.....	23
4	Basic Setup	25
4.1	Retrieve System Information via gladm	25
4.2	Verify the Authenticity of the Device (Standard FIPS).....	26
4.3	Change Default Credentials of OPERATOR.....	28
4.4	Create a new cHSM	31
5	Global Administration	34
5.1	Set Device Time.....	34
5.2	Generate an Operator Secret	34
5.3	Import an Operator Secret	36
5.4	Copy an Operator Secret.....	39
5.5	Managing the MBK on u.trust Anchor	41
6	Contact Address for Support Queries	43
7	References	44

1 Introduction

This document provides step-by-step instructions on how to bring the u.trust Anchor LAN into service, how to prepare a computer for the u.trust Anchor LAN administration, and guides you through the initial administration steps for the u.trust Anchor device.

This guide is intended as a supplement to the documentation provided in the product bundle.

The product bundle is downloadable from the following site:

<https://support.hsm.utimaco.com/support/downloads/>



You have to be registered for this download portal and access to a download area, e.g., „SecurityServer Se Gen2“, must have been granted.

For detailed information on the full range of setup and configuration options, please read the [u.trust Anchor LAN V5 FIPS 140-3 - Administration Manual](#) and the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

Before you start with the installation, please read the topic *General Safety Instructions* in the [u.trust Anchor LAN V5 FIPS 140-3 - Operating Manual](#) and examine the u.trust Anchor LAN device for obvious signs of damage.



To immediately begin setup procedures, please navigate to the [Getting Started](#) chapter.

1.1 Security Guidelines

1.1.1 General Advice

We highly recommend using strong passwords consisting of at least eight random characters, which should include uppercase and lowercase letters, special characters, and random numbers.

Keep the passwords secret, do not write them down anywhere, and change them regularly.

We highly recommend regularly checking the state of the battery.

1.1.2 Protected Operational Environment

Before you start operating the device, ensure that the system environment is highly secure by checking that:

- No secure seal is damaged.
- The PIN, PUK or password entry cannot be monitored.
- The device is securely stored and appropriately protected against unauthorized access.
- The PIN pad is securely stored, if purchased.
- The smartcards are securely stored, if purchased.
- Only trustworthy persons have physical-/network access.
 - The administration and configuration/setup of the u.trust Anchor shall be exclusively done by verified, trusted, authorized, and well-trained persons.
- Only authorized changes to the software and the configuration of the device are possible.
- Regular inspections are required to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the u.trust Anchor).
- The u.trust Anchor must be protected against the possibility of attacks that are based on emanations, like electromagnetic emanations or Simple Power Analysis (SPA) or Differential Power Analysis (DPA) attacks.

Additional measures for operating an u.trust Anchor PCIe card/using an administration computer with the client application:

The following information is relevant for operating an u.trust Anchor PCIe card, and for any host PC/server where the u.trust Anchor PCIe card is integrated and in which Utimaco host APIs and tools are running:

- Only trustworthy persons have physical and network access to the u.trust Anchor and to the administration computer.
 - The administration and configuration/setup of the administration computer shall be done exclusively by verified, trusted, authorized, and well-trained persons.
- The administration computer in which the u.trust Anchor PCIe card is installed shall be placed in a highly secured area that can be only reached by authorized people.

Unauthorized persons shall not have any access to the administration computer. It shall be secured by an access control mechanism, for example, a password and/or smartcard.

- The following rules apply for the passwords:
 - The minimum recommended password length is eight characters.
 - The password shall contain uppercase and lowercase letters, at least two special characters, and numbers.
 - The password shall be changed periodically – at least every three months.
- The administration computer shall be checked for malware prior to installing the u.trust Anchor card and the administration tools. Software that is not trustworthy and not required for the operation and administration of the u.trust Anchor shall be uninstalled.
- An antivirus software with the latest updates shall be installed and running on the administration computer.
- We highly recommend using the administration computer exclusively for the operation and administration of the u.trust Anchor. There should be no Internet access and remote computer administration should be restricted to a minimum.

1.1.3 Protection of Data Outside the u.trust Anchor

- Any externally stored data must be protected against loss, theft, unauthorized access, and modification. This includes the following data:
 - For any cHSM, the MBK that is used for creating a backup of the keys of a cHSM.
 - The backup copies of cryptographic keys or user backups.
 - Keys that are exported from the u.trust Anchor and keys that shall be imported into the u.trust Anchor.
 - Your Operator Base Secret (OBS).
 - The certificates of the Device Authentication Key (DAK) and any Container Authentication Key (CAK).
 - The audit data that are exported from the u.trust Anchor.
 - The private authentication keys of the users that are registered on the u.trust Anchor and are either stored in keyfiles or on smartcards.

- Any backups should be maintained in a way that ensures appropriate controls over making backups, storing backup data, and using backup data to restore an operational u.trust Anchor. The number of sets of backup data shall not exceed the minimum needed to ensure continuity of the required services.

2 Overview

The u.trust Anchor HSM is a multi-tenant Hardware Security Module (HSM) platform for payment and general-purpose use cases that enables cloud service providers and enterprises to offer HSM-as-a-Service (HSMaaS).

The u.trust Anchor HSM offers up to 31 cHSMs (containerized Hardware Security Modules) and multiple PKCS #11 partitions per cHSM for application separation and key partitioning. Each cHSM instance is isolated; the administrative access and cryptographic functions are limited to the corresponding cHSM user, ensuring the required level of confidentiality for their sensitive data and keys.

A clear separation is maintained between the Global Administrator (see *Roles* in the [u.trust Anchor - Administration Manual](#)) who orchestrates the physical HSM and the overall setup, and the cHSM Administrators (see *Roles* in the [u.trust Anchor - Administration Manual](#)) who manage their corresponding virtual cHSMs. For further details, see [Architecture](#).

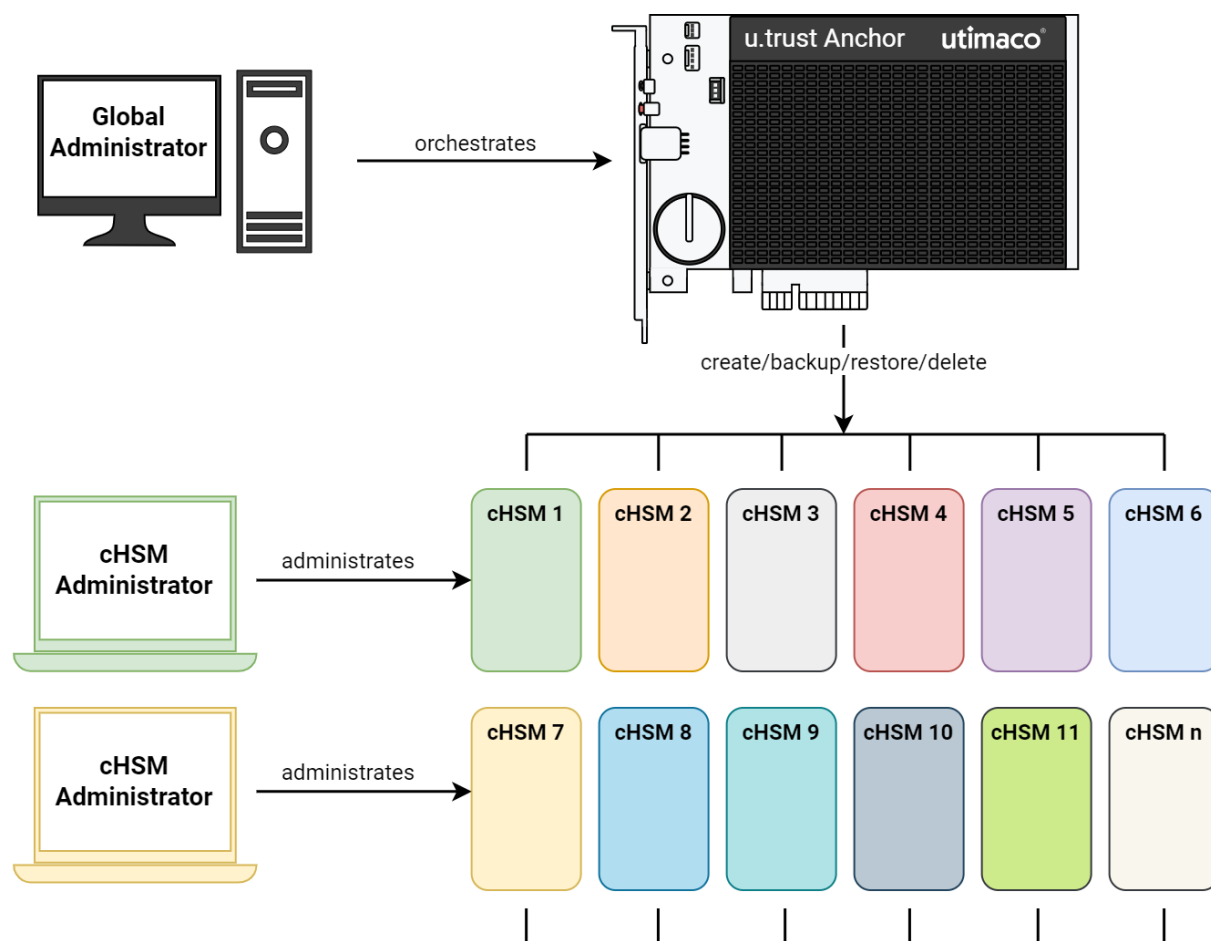


Figure 1 : u.trust Anchor and cHSMs

Various templates are provided for the creation of cHSMs; the cHSMs will have varying attributes and functionalities, depending on the template chosen.

The u.trust Anchor platform offers the following core features:

- Usage of up to 31 cHSMs (containerized Hardware Security Modules)
For information on which product supports how many cHSMs, see [u.trust Anchor Product Line](#).
- Key management
- Key usage
- Certificate management
- Storage

- Encryption

These core functions are performed within a tamper-resistant, hardened environment, guaranteeing the integrity and confidentiality of sensitive data. The critical hardware components of a u.trust Anchor are located on a printed circuit board, completely covered by potting material. This hard, opaque enclosure protects the sensitive u.trust Anchor hardware components from physical attacks. If the sensory controller (powered by the on-board battery) detects a critical tamper event (see *Alarm Triggers* in the [u.trust Anchor - Administration Manual](#)), all sensitive information is deleted immediately. For further details, see *Alarm Mechanism* in the [u.trust Anchor - Administration Manual](#).

For an extended overview, see *Overview* in the [u.trust Anchor - Administration Manual](#).

2.1 Architecture

The u.trust Anchor has two administration categories:

1. The orchestration of the physical u.trust Anchor HSM, including basic management (creation, backup, restore, and deletion) of all cHSMs (virtual containerized Hardware Security Module)
 - The Global Administrator (see *Roles* in the [u.trust Anchor - Administration Manual](#)) issues commands via gladm (Global Administration Management tool, see *gladm* in the [u.trust Anchor - Administration Manual](#)), which are communicated by the Global Administration (glad) service to Gladracks (container orchestration system, see *Software* in the [u.trust Anchor - Administration Manual](#)) and are executed within the device.
 - The entity operating and owning the physical u.trust Anchor HSM is called the OPERATOR (see *Roles* in the [u.trust Anchor - Administration Manual](#)).
2. The administration of a virtual cHSM (containerized Hardware Security Module)
 - The cHSM Administrator (see *Roles* in the [u.trust Anchor - Administration Manual](#)) issues commands via the cHSM Toolset (see *Toolset* in the [u.trust Anchor - Administration Manual](#)), which are executed by the cHSM firmware within the container.
 - The programs of the cHSM Toolset (see *cHSM Toolset* in the [u.trust Anchor - Administration Manual](#)) can either communicate directly with a cHSM (*csadm* and *cxitool*, see *csadm* and *cxitool* in the [u.trust Anchor - Administration Manual](#)) or via a range of standard APIs (PKCS#11, CNG, OpenSSL JCE).

- The entity operating (and owning) the virtual cHSM is called a cHSM TENANT (see *Roles* in the [u.trust Anchor - Administration Manual](#)).



The (secret) data stored in each cHSM is isolated within the container and cannot be accessed by the Global Administrator (see *Roles* in the [u.trust Anchor - Administration Manual](#)) or another cHSM.



The OPERATOR (see *Roles* in the [u.trust Anchor - Administration Manual](#)) and the cHSM TENANT (see *Roles* in the [u.trust Anchor - Administration Manual](#)) can belong to the same or different organizations.



The VENDOR (Utimaco), see *Roles* in the [u.trust Anchor - Administration Manual](#), can only access the u.trust Anchor during the manufacturing process or in case of a Return Merchandise Authorization (RMA).

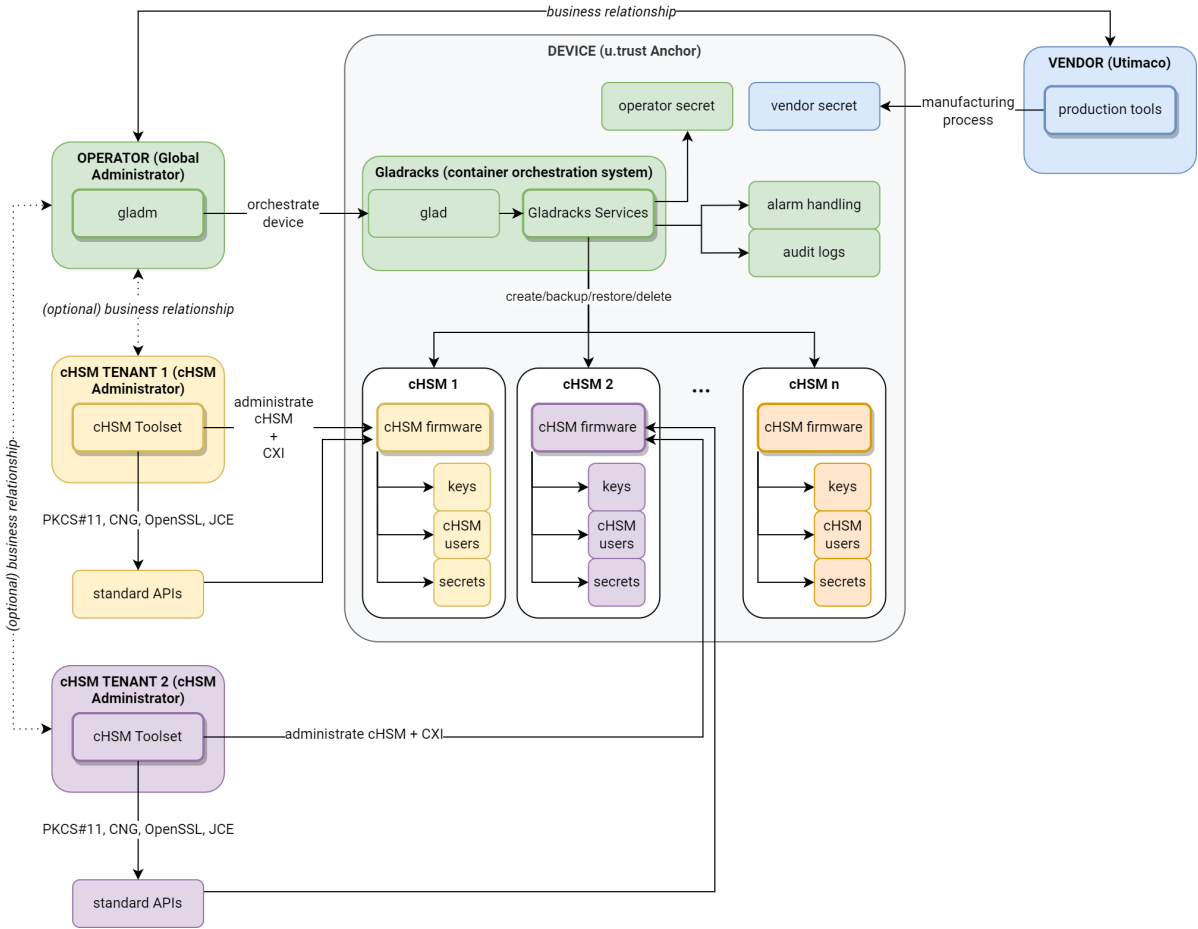


Figure 2 : u.trust Anchor - Architecture

2.2 Templates

The u.trust Anchor provides templates for the creation of cHSMs. Depending on which template is used to create a cHSM, it has different attributes and functionalities. All templates support the usage of an alternative module signature key (AMSK) to load a custom firmware module.

Template	Description	Standard Package	FIPS Package (certifiable)	GP CC Package (certifiable)
SecurityServer	Creates a standard cHSM.	✓	✓	✓
SecurityServer-SDK	Creates an SDK cHSM.	✓	✗	✗

Template	Description	Standard Package	FIPS Package (certifiable)	GP CC Package (certifiable)
SecurityServer-FIPS	Creates a <i>FIPS cHSM</i> according to the standards defined in FIPS-140-3. FIPS cHSMs block a number of functions, see section <i>Availability of Commands in FIPS mode</i> in <i>u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (cHSM) - Administration Manual</i> .	✓	✓	✗
SecurityServer-FIPS-SDK	The FIPS-SDK template is the merge between the SDK and FIPS templates. It has the SDK behavior plus FIPS restrictions.	✓	✗	✗
SecurityServerCC	Creates a <i>CC cHSM</i> according to the standards defined in Common Criteria (EAL4+).	✗	✗	✓

Table 1: Templates



SDK templates are only available with a valid u.trust Anchor SDK license.



In this manual, all further mentions of *cHSM* refer to all kinds of cHSMs, and all specific differences are pointed out by stating the respective information for *SDK cHSMs* where applicable.

2.3 u.trust Anchor Product Line

u.trust Anchor is offered as a single PCIe card or mounted in a LAN appliance.

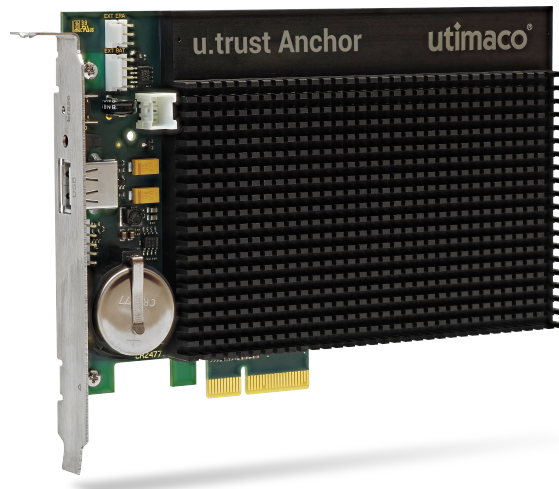


Figure 3 : u.trust Anchor PCIe card



Figure 4 : LAN Appliance Front View

Available models:

Product	Model Number	cHSMs	RSA 2k Performance	Certification	Certification Status
u.trust Anchor Se	Se100	1	100	FIPS 140-3 Level 3	In progress
	Se2k	4	2000	FIPS 140-3 Level 3	In progress
	Se5k	8	5000	FIPS 140-3 Level 3	In progress
	Se15K	4	15000	Common Criteria EAL4+ FIPS 140-2 Level 3 FIPS 140-3 Level 3	Certified (v.4.49.0) Certified (v.4.47.2) In progress
	Se40K	12	40000	Common Criteria EAL4+ FIPS 140-2 Level 3 FIPS 140-3 Level 3	Certified (v.4.49.0) Certified (v.4.47.2) In progress
u.trust Anchor CSAR	Standard	8	40000	Common Criteria EAL4+ FIPS 140-2 Level 3 FIPS 140-3 Level 3	Certified (v.4.49.0) Certified (v.4.47.2) In progress

<i>Product</i>	<i>Model Number</i>	<i>cHSMs</i>	<i>RSA 2k Performance</i>	<i>Certification</i>	<i>Certification Status</i>
	Plus	12	40000	Common Criteria EAL4+ FIPS 140-2 Level 3 FIPS 140-3 Level 3	Certified (v.4.49.0) Certified (v.4.47.2) In progress
	Premium	31	40000	Common Criteria EAL4+ FIPS 140-2 Level 3 FIPS 140-3 Level 3	Certified (v.4.49.0) Certified (v.4.47.2) In progress

Table 2: Hardware Models



To upgrade your u.trust Anchor model, the device needs to be sent back to Utimaco to perform the upgrade. In-field upgrade licenses will be enabled in a future release.

3 Getting Started

In the following description, it is assumed that administration of the u.trust Anchor LAN V5 device will be carried out on an administration computer.

3.1 Switch on the u.trust Anchor LAN



Figure 5 : u.trust Anchor LAN V5 Front View

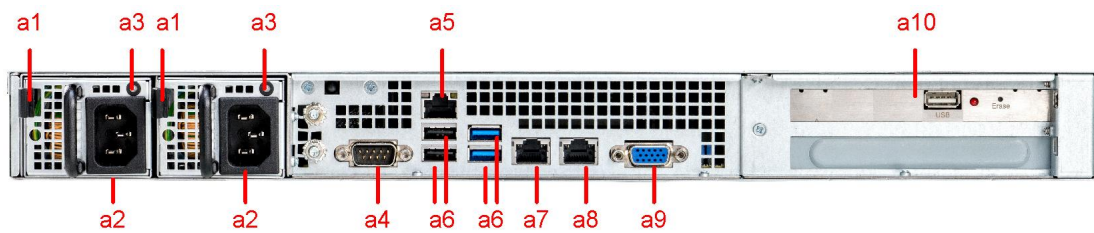


Figure 6 : Rear View

1. Connect the power supply sockets (a2) on the rear side of u.trust Anchor LAN to a power supply using the cables supplied with the device.
2. Connect the **eth0** (a7) ethernet port on the rear side of the u.trust Anchor LAN to your installation network with a twisted pair cable (RJ45).
3. Press the on/off switch on the front panel.

After a few seconds you will hear a short signal tone and the first messages are displayed. After approximately 90 seconds, the u.trust Anchor LAN is ready for use and status information is displayed through alternating display screens:

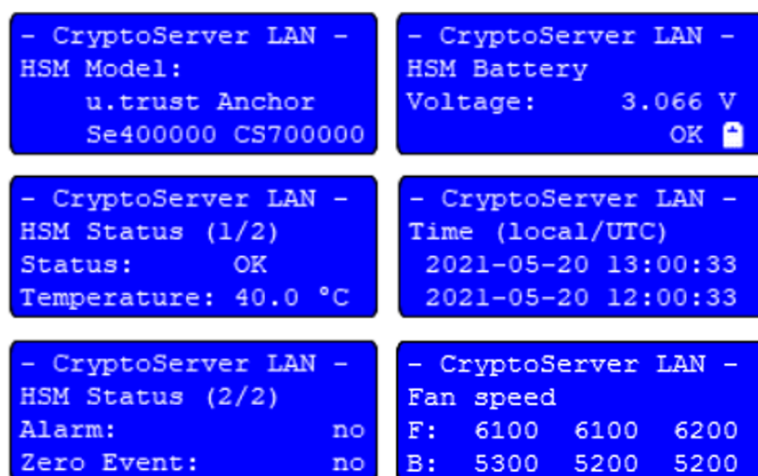


Figure 7 : Idle Screens

- **HSM Model:** The u.trust Anchor model and the unique serial number of the u.trust Anchor PCIe card.
- **HSM Battery Voltage:** The voltage and the status of the carrier battery.
- **Temperature:** The current temperature of the u.trust Anchor in °C.
- **Time (local/UTC):** The local time and the UTC (Coordinated Universal Time) of the u.trust Anchor LAN (not of the u.trust Anchor PCIe card).
- **HSM Status:** The status will read as 'OK' if there is no alarm and no zeroization event.
- **Fan Speed:** A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return Merchandise Authorization) according to the Chapter "Contact Address for Support Queries".

4. Ensure the **HSM Status** display shows **Status: OK**.

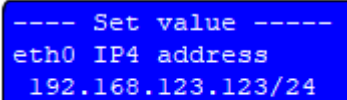


The u.trust Anchor LAN is switched on and ready for setup.

3.2 Configure the IP Address (e.g., static IPv4)

1. Press **ENTER** on the front panel of the device.

2. Press **ENTER** to select **CSLAN admin**.
3. Press **ENTER** again to select **Configuration**.
4. Select **Network IP4** and press **ENTER**.
5. Select **eth0** and press **ENTER**.
6. Use the **↓** key to select **Address** and press **ENTER**.
7. Enter the IP address of the LAN device by using the **↑** **→** **↓** **←** keys. Then press **ENTER**, the **→** key and **ENTER** again to confirm.



```
----- Set value -----  
eth0 IP4 address  
192.168.123.123/24
```

Figure 8 : IP Configuration

- ↑, ↓** : Change the displayed digit
←, → : Change the cursor position



The IP address has been configured successfully.

3.3 Configure the IP Address for the Default Gateway

1. Press **ENTER** on the front panel of the device.
2. Press **ENTER** to select **CSLAN admin**.
3. Press **ENTER** again to select **Configuration**.
4. Select **Network IP4** and press **ENTER**.
5. Use the **↓** key to select **Default gateway** and press **ENTER**.
6. Enter the IP address of the default gateway by using the **↑** **→** **↓** **←** keys. Then press **ENTER**, the **→** key and **ENTER** again to confirm.

```
---- Set value ----  
Default gateway  
192.168.123.123
```

Figure 9 : IP Address for the Default Gateway

↑, ↓ : Change the displayed digit

←, → : Change the cursor position



The IP address for the default gateway has been configured successfully.

3.4 Enable the SSH Daemon

To enable the Secure Shell (SSH) daemon to set up remote SSH access, do the following:



Since the SSH daemon is enabled by default, these steps are only needed if it has been disabled.

1. Press **ENTER** on the front panel of the device.
2. Press **ENTER** to select **CSLAN admin**.
3. Press **ENTER** again to select **Configuration**.
4. Press the ↓ key to select **Services** and confirm by pressing **ENTER**.
5. Press **ENTER** to select **SSH**.
The currently applied setting (**disabled** or **enabled**) is indicated by a full circle.
6. Use the ↓ key to select **enabled** and press **ENTER** to open the menu item.
7. Use the ← or the → key to move the x into the brackets **[x] Yes** and press **ENTER**.



A message is displayed confirming that you have successfully enabled SSH.

3.5 Preparation Steps on the Administration Computer

3.5.1 Install Java

1. Download and install the Java Runtime Environment (JRE): <http://java.com/en/download/>
2. Download the corresponding Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files (e.g., `jce_policy-8.zip`), extract them, and copy the `.jar` files to `<your Java installation directory>\lib\security`. The existing `.jar` files in the directory are overwritten.

3.5.2 Install gladm

gladm is a tool used by the Global Administrator to perform administrative tasks on the u.trust Anchor device.

Installing gladm on a computer with a Windows operating system

This section describes how to install gladm on a Windows administration computer.


On an administration computer running a Windows operating system, gladm is installed by default during the installation of the u.trust Anchor software provided in the product bundle.

The following steps describe how to install gladm on a Windows host computer.

You will find the `gladm.exe` file for Windows in the product bundle here:

- For Windows 32-bit operating systems
Not supported
- For Windows 64-bit operating systems
`Software\Windows\Administration\`

1. Copy the `gladm.exe` file to a well-chosen directory.
2. Add this directory to the `PATH` environment variable to be able to call the Administration Tool from any other directory.

 gladm has been successfully installed on the administration computer.

Installing gladm on a computer with a UNIX-like operating system

This section describes how to install gladm on a Linux administration computer.

The gladm installation file is provided within the product bundle under `.../Software/Linux/Administration`.

1. Create a `~/bin` directory in your user directory, if there is not one yet:

```
mkdir ~/bin
```

2. Copy the gladm relevant for your operating system into the `~/bin` directory. An example for Linux 64-bit:

```
cp <mount point of the product bundle>/Software/Linux/Administration/gladm  
~/bin
```

3. Ensure that you have write and execute permissions for gladm.

```
chmod -R u+w+x ~/bin
```

4. Add the `~/bin` directory to the path in the user configuration file in the shell that is being used. In this example, a bash is used as the shell, i.e., open the `~/.bashrc` file and add the following line to it:

```
export PATH=$PATH:~/bin
```

5. Save the changes and close the `~/.bashrc` file.

 gladm has been successfully installed on the administration computer.

3.5.3 Install csadm

csadm is used to manage cHSMs on the u.trust Anchor device.

Installing csadm on a computer with a Windows operating system

This section describes how to install csadm on a Windows administration computer.

On an administration computer running a Windows operating system, csadm is installed by default during the installation of the u.trust Anchor software provided in the product bundle.

The following steps describe how to install csadm on a Windows host computer.

The `csadm.exe` file for Windows can be found in the product bundle here:

- For Windows 32-bit operating systems
Not supported
- For Windows 64-bit operating systems
`Software\Windows\Administration\`

1. Copy the `csadm.exe` file to a well-chosen directory.
2. Add this directory to the `PATH` environment variable to be able to call the administration tool from any other directory.



csadm has been successfully installed on the administration computer.

Installing csadm on a computer with a UNIX-like operating system

This section describes how to install csadm on a Linux administration computer.

The csadm installation file is provided within the product bundle.

1. Create a `~/bin` directory in your user directory, if there isn't one yet:

```
mkdir ~/bin
```

2. Copy the csadm relevant for your operating system into the `~/bin` directory. An example for Linux 64-bit:

```
cp <mount point of the product CD>/Software/Linux/Administration/csadm ~/bin
```

3. Ensure that you have write and execute permissions for csadm.

```
chmod -R u+w+x ~/bin
```

4. Add the `~/bin` directory to the path in the user configuration file in the shell that is being used. In this example, a bash is used as the shell, i.e., open the `~/.bashrc` file and add the following line to it:

```
export PATH=$PATH:~/bin
```

5. Save the changes and close the `~/.bashrc` file.



csadm has been successfully installed on the administration computer.

3.5.4 Log in Remotely and Change the Default Password

Prerequisites

- An IP address must have been assigned to the u.trust Anchor, see [Configure the IP Address \(e.g., static IPv4\)](#).
- The SSH daemon is enabled by default. If it has been disabled, enable it; see [Enable the SSH Daemon](#).

To change the password for the `root` and `csagent` user by logging in remotely to the u.trust Anchor LAN, proceed as follows:

1. Start your SSH client (for example, PuTTY or WinSCP on Windows or ssh on Linux).
2. Log in to your u.trust Anchor LAN via SSH with the following access data:

```
Host name = <computer name/IP address of the u.trust Anchor LAN>  
Port number = 22
```

```
User name/CryptoServer login = cslagent
```

```
Password = utimaco
```

3. To change the password for the `root` or `cslagent` user, enter `passwd` and press **Enter**.
4. Enter the old password.
5. Enter the new password.



Make sure the password consists of at least six characters. It must be a combination of lower case letters, upper case letters, and numbers.

6. Log out from u.trust Anchor LAN with the `exit` command.
7. Perform the exit command once more.



The password has been successfully changed.

4 Basic Setup

This section describes the required steps to set up a cHSM on the u.trust Anchor device. After a cHSM has been created, the cHSM Administrator can use it for further configuration.

Two steps are required to complete the cHSM setup:

- Replace the pre-installed Global Initial Authentication Key (GIAK) of the OPERATOR with the Global Admin Authentication Key (GAAK) to get full access to OPERATOR functionality. See [Change Default Credentials of OPERATOR](#).
- Create a cHSM. During this process, the OPERATOR loads the public key of the default cHSM administrator. See [Create a new cHSM](#).

Once the cHSM is created, the cHSM Administrator can log in to the cHSM with the associated secret key.

4.1 Retrieve System Information via gladm

First, check that system information can be retrieved from the device via the `gladm system-get-info` command:

```
gladm -d <device> system-get-info
```



A device can be addressed using either the IP address or hostname of the u.trust Anchor LAN device:

- Examples:

- `gladm ... -d 123.123.123.123 -p 4000 ...`
- `gladm ... -d myPC -p 4000 ...`

The optional `-p` argument indicates the port that is used on the computer or LAN device. Default if this argument is not set: 4000.

The output should contain the following lines and should not contain any alarms or zeroization events:

```
Initial user credentials unchanged
No alarm present
No zeroization event occurred
```

Vendor Secret is present on the device
Vendor DAK Certificate is present on the device

Before starting the setup, you should also verify the authenticity of the device, see (1.0.5) 2023-0034 Verify the Authenticity of the Device - CHECK.

4.2 Verify the Authenticity of the Device (Standard | FIPS)

When setting up the device for the first time, you should perform the following steps to ensure the authenticity of the device before uploading your certificates.



Note that this step is optional. It is necessary if you want to verify the HSM is genuine and manufactured by Utimaco. This step is expressly recommended from a safety perspective.

To perform the following commands, the device needs to be addressed correctly as described in *Specifying a Device* in the *u.trust Anchor - Administration Manual*, where the placeholder `<device>` is given.

1. Get the system information via the `gladm system-get-info` command, see the *Displaying Device System Information (system-get-info)* chapter of the *u.trust Anchor - Administration Manual*.

```
gladm -d <device> system-get-info
```

The output should contain the following lines:

```
Initial user credentials unchanged  
No alarm present  
No zeroization event occurred  
Vendor Secret is present on the device  
Vendor DAK Certificate is present on the device
```

2. Use the Utimaco root certificate `u-trust-Anchor-ROOT-CA-1.cer` that is delivered within the product bundle at `/Software/Linux/Administration/key` (for Windows: `\Software\Windows\Administration\key`) as an additional verification parameter in a `gladm` command, for example with the command `gladm system-get-info`.

```
gladm -d <device> --vendor=u-trust-Anchor-ROOT-CA-1.cer -u admin -k giak.pem  
system-get-info
```

By using the `--vendor=` parameter with the Utimaco root certificate in combination with the Global Administrator authentication credentials, the command checks the given certificate against the vendor certificate stored on the device. If the command is executed successfully, the certificate is verified. In case the certificate is not verified, an error is returned and the command is not executed. In this case, contact Utimaco immediately.



The device has been verified successfully as a genuine Utimaco u.trust Anchor device that has not been tampered with.

Verification by the operator can always be done by retrieving the relevant certificates via `gladm system-get-trust-chain` and verifying them with openssl:

1. Retrieve the chain of trust. For authentication, use the Global Initial Admin Key that is delivered within the product bundle at `/Software/Linux/Administration/key` (for Windows: `\Software\Windows\Administration\key`).

```
gladm -d <device> -u admin -k giak.pem system-get-trust-chain
```

The Certificate Signing Request is returned along with all available certificates.

```
device auth key certificate signing request written to: device-auth-key.csr  
operator device auth key certificate chain not present  
vendor device auth key certificate chain written to: dak-vendor-chain.pem  
glad auth key certificate written to: glad-auth-key-device-cert.pem
```



In DAK and GAK certificates, Elliptic Curve (EC) point compression is used. This is an optional feature according to the corresponding standards and is not necessarily supported by all tools.

2. Take the DER-coded root certificate `u-trust-Anchor-ROOT-CA-1.cert` supplied to you within the product bundle at `/Software/Linux/Administration/key` (for Windows: `\Software\Windows\Administration\key`) and convert it to a PEM-formatted file

named `Utimaco_root.pem` via openssl.

```
openssl x509 -in u-trust-Anchor-ROOT-CA-1.cer -inform DER -out
Utimaco_root.pem
```

3. Verify the chain by using the converted Utimaco root certificate and the vendor certificate from the trust chain.

```
cat <path>/u-trust-Anchor-ROOT-CA-1.pem dak-vendor-chain.pem | openssl
verify
```

The following line should be returned:

```
dak-vendor-chain.pem:OK
```



The verification with openssl can occasionally return some openssl errors (e.g. error 20 at 0 depth lookup: unable to get local issuer certificate). In case this happens, use gladm to verify the certificates.

Before starting regular use, make sure to update the device using the latest FIPS certified system image available, see *Updating the Device Firmware (system-update) in the u.trust Anchor FIPS 140-3 - Administration Manual*.

4.3 Change Default Credentials of OPERATOR

The purpose of this step is to replace the default Global Initial Authentication Key (GIAK) with a Global Admin Authentication Key (GAAK), which is generated and owned by the OPERATOR.

The Global Initial Authentication Key (GIAK) (`giak.pem`) is delivered within the product bundle at `/Software/Linux/Administration/key` (for Windows: `\Software\Windows\Administration\key`). This initial key only provides access to a very restricted set of commands and must be replaced.



Only the following commands (and those that do not require user authentication at all) can be executed using GIAK:

- `user-change-credentials`
- `system-get-trust-chain`
- `system-reset-alarm`

When the execution of a command/function requires authentication and GIAK was not replaced, the HSM returns the error message, "The user authentication key needs to be updated".



Note that some commands like `system-get-info` do not require user authentication at all. For more information, see the *Changing Requirements for Dual Control* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

A list of users can be generated using the command `user-list`. The optional parameter `-v` generates a list of permissions for each user:

```
gladm -d <device> user-list -v

admin                - [
system_get_trust_chain
system_reset_alarm
user_change_credentials
]
```

Creating the GAAK

The GAAK can be created using the Utimaco csadm administration tool as shown below. It is advisable to generate and store the GAAK key pair on smartcards for production environments. Only the public key is loaded into the HSM for Global Administrator authentication.



When the u.trust Anchor device starts for the first time after delivery or after having been cleared, the role of the Global Administrator is that of the Global Initial Administrator ADMIN.

Example for a key generation with csadm directly on a smartcard:

```
csadm keytype=EC genkey=:cs2:auto:USB0,admin
-> generating EC key: :cs2:auto:USB0, curve brainpoolP320t1, owner: admin
```

Example with a key file and EC algorithm:

```
csadm KeyType=EC genkey=GAAK.key,ADMIN
-> generating EC key: CustomerIAK.key, curve brainpoolP320t1, owner: ADMIN
```

Example with a key file and RSA algorithm:

```
csadm KeyType=RSA genkey=GAAK.key,2048,ADMIN
-> generating RSA key: CustomerIAK.key, 2048 bits, owner: ADMIN
```

Replacing the GIAK with the GAAK

To acquire full initial admin rights, the GIAK key must be replaced with GAAK. In order to replace the GIAK and load the GAAK public key into the HSM, perform the command `gladm user-change-credentials`, authenticating it with the GIAK secret key (giak.pem) from the product bundle.

Example of changing credentials with a smartcard:

```
gladm -d <device> -u admin -k giak.pem user-change-credentials
admin :cs2:auto:USB0
Changing user credentials with parameters:
  user name: admin
  public key: :cs2:auto:USB0
```

Example with a key file:

```
gladm -d <device> -u admin -k giak.pem user-change-credentials admin GAAK.key
Changing user credentials with parameters:
```

```
user name: admin
public key: GAAK.key
```



Before beginning regular use, be sure to update the device using the latest system image available. See *Updating the Device Firmware (system-update)* in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

4.4 Create a new cHSM

Prerequisites

Have the public part of the Container Administration Authentication Key (CAAK) at hand that is supplied by the cHSM TENANT who will use the cHSM.

If CUSTOMERs do not yet have a key, they must generate a key pair and save the public part in a place where it can be accessed.

The most secure and therefore recommended way to generate a private key is to use `csadm GenKey` to generate an RSA key pair (private and public key) on a smartcard and then save the public key with `csadm SaveKey`. For details see, *GenKey* and *SaveKey* in the *u.trust Anchor csadm Manual*.

```
csadm GenKey=:cs2:cjo:USB0,"cHSM User"
Generates an RSA key pair on the smartcard.
```

```
csadm PubKey=:cs2:cjo:USB0 SaveKey=C:\keys\pubkey1.key
Extracts the RSA public key from a smartcard and stores it in a file.
```

Procedure

1. Execute the `gladm chsm-create` command. The only required parameters are the admin key file and the slot ID within the u.trust Anchor device. If no other parameters are given, the new cHSM will be created using the default template. The resulting certificates will be stored in the working directory.

Example to create a new cHSM in slot 15 with the public key part `myADMIN.pub` used as initialization data:

```
gladm -d <device> -u admin -k admin_gaak.pem chsm-create myADMIN.pub 15
Creating cHSM...
slot: 15
```

```
init_data: myADMIN.pub
```

Depending on the device type you use, the specified cHSM slot might not exist (in the example: slot 15). In this case, the following error message is shown:

```
Operation failed: CHAI_SLOT_INVALID: The requested cHSM slot is invalid or
unavailable
```

In this case, perform a `gladm chsm-list-slots` command to show the available cHSM slots and repeat the `gladm chsm-create` command using one of the available cHSM slots.

2. When the command is performed, u.trust Anchor creates a Container Authentication Key (CAK), which is then signed with the Device Authentication Key (DAK), allowing the cHSM to prove it runs on genuine hardware.

While executing this action, u.trust Anchor writes the following files:

- the cHSM creation receipt, containing the Container Administration Authentication Key (CAAK) used to set up the cHSM along with a timestamp and the cHSM's UUID;
- a CSR for the Container Authentication Key (CAK) to be signed by the customer;
- the certificates for the vendor signed certificate of the Device Authentication Key (DAK);
- the DAK-signed certificate of the CAK and the GlAD Authentication Key (GAK), and
- the operator-signed certificate of the DAK.

Output pattern

```
cHSM creation receipt... .txt
cHSM receipt signature...
cSHM auth key certificate... .csr
device cHSM auth key certificate written to... .pem
glad auth key cert... .pem
vendor device auth key... written to... .pem
operator device... written too... .pem
```

3. Provide the u.trust Anchor cHSM Administrator with these files so that they are able to claim the u.trust Anchor cHSM.



The u.trust Anchor cHSM has been successfully created and can be verified and claimed by the u.trust Anchor cHSM Administrator.

To create additional cHSMs and use snapshots, one must first load the operator secret into the HSM. See [Generate an Operator Secret](#) for more information.

If only one cHSM will be utilized and if the snapshot option is not used, the cHSM administrator can begin the configuration of the cHSM. Backups can still be performed inside the cHSM (i.e. backup of the user database and key database via CSADM or CAT).

5 Global Administration

5.1 Set Device Time

Perform the `gladm system-get-time` command and compare the returned time to your local system time. For more information on this command, see the *Getting the Time* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

```
gladm -d <device> system-get-time
```

The date and time of the device are returned in the `YYYY-MM-DD HH:MM:SS` format.

```
2022-05-29 18:35:29 UTC
```

In case the time of the device differs, perform the `gladm system-set-time` command without any further parameters. For more information on this command, see the *Setting the Time* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

```
gladm -d <device> system-set-time
```

The device time is set to the local system time.

```
Set system time with parameters:  
time: 2022-06-15 17:58:06 UTC
```

5.2 Generate an Operator Secret

Operator secrets are used alongside a vendor secret to derive keys used for the encryption of snapshots. This approach prevents either party from decrypting any of the created snapshots.

A snapshot contains the data of a cHSM stored on disk at the time of taking the snapshot. It contains the user data created after the cHSM was created. Snapshots can be taken of running, halted, or locked cHSMs. When taking a snapshot of a running cHSM, the cHSM is temporarily halted and remains unavailable until the snapshot operation has been completed. Taking snapshots of cHSMs in cluster mode is not supported.

An operator secret consists of 32 bytes and is generated and stored securely by the operator. u.trust Anchor additionally offers the possibility to import wrapped operator secrets.

An operator secret must be loaded onto the device to create multiple cHSMs, and at least one active operator secret is necessary to create snapshots. The device can store multiple operator secrets, of which at most one can be active. The active secret is used when new snapshots are created. The other secrets are used to import snapshots that were created by using those secrets.



Global Administrators should use a dedicated smartcard for operator secrets (and not use the same smartcard for MBKs, for example).

Procedure:

1. Connect the smartcard reader to the device and insert the smartcard.
2. Generate an operator secret via `gladm key-set-operator-secret`. In this example `-g` generates the operator secret, splits it into 3 shares out of which 2 are needed to recover the secret. The share is saved on position 7 on the smartcard.

```
gladm -u admin -k admin_gaak.pem key-set-operator-secret -g 2,3 -r 7 :cs2:auto:USB0
```



The command cannot be executed if an operator secret is already present on the smartcard. Use `[-f]` to overwrite the existing record on the smartcard.

```
gladm -u admin -k admin_gaak.pem key-set-operator-secret -g 2,3 -f -r 7 :cs2:auto:USB0
```

3. The command is executed once and a message on the PIN pad will be displayed, telling you when to press OK and when to insert the next card.
4. The shares are saved on the smartcards. A wrapping key is obtained from the device, and the operator secret is wrapped and imported into the u.trust Anchor.
5. Check the operator secret list via `gladm key-list-operator-secrets`.

```
gladm -u admin -k admin_gaak.pem key-list-operator-secrets
```

6. Upon successful execution of the command, gladm returns a list of the available operator secrets, along with the file date. The new operator secret will become the active operator secret. The previous operator secret will remain available for loading user backups and snapshots.

```
646d4110: 2021-06-24T12:26:21+0000 - active
fecf521a: 2021-06-24T12:26:16+0000
da1bcbb3: 2021-06-24T12:26:12+0000
```

5.3 Import an Operator Secret



This step is not mandatory, however, it is required if you have to instantiate more than one cHSM. The operator secret must be loaded to allow the creation of snapshots and to restore cHSMs.

An operator secret must be imported to enable the taking and restoring of snapshots. All snapshots created on a device with an active operator secret can be restored on all devices that hold this specific operator secret.



The operator secret alone is not sufficient to get access to the cHSM snapshot data. Namely, the vendor secret – which is loaded into the HSM during production – and the operator secret are combined to derive snapshot protection keys. Though, neither the OPERATOR nor the manufacturer can access the data in the snapshot.

The operator secret is imported into the device with the `gladm key-import-operator-secret` command. The last imported operator secret will be set as active and will be used in subsequent calls that create a snapshot on this device. In case there is an inactive copy of the operator secret already present on the device, the inactive copy has to be deleted first before re-importing.

1. Use `gladm` to check if an operator secret is present on the device.

```
gladm -d <device_IP> -u <username> -k <credentials> key-list-operator-secrets
```


No Operator Secret present.

2. Generate a key wrapping key (KWK).

The HSM will generate a public and private key and will give you back the public key (in the form of a certificate signed by the DAK key) as the response. The provided token will be used during the export to identify the KWK.



Note that the KWK is a one time use key. The purpose of that key is to securely load the operator secret into the HSM. The operator secret is cryptographically wrapped by the public part of the KWK and unwrapped in the HSM with the corresponding private key.

Use `--vendor` (or if already established, `--operator`) to authenticate the device against the Utimaco root certificate (or OPERATOR root certificate) since the given public key will be used to wrap the operator secret. Furthermore, the exporting system should verify the KWK certificate chain against the corresponding CA as well.

```
gladm -d <device_IP> --vendor=ROOT_CA.cer -u <username> -k <credentials>  
key-get-wrapping-key -c <wrappingkeyname> -t <tokenID> <keysize>
```

```
example : gladm -d 10.17.72.6 --vendor=u-trust-Anchor-ROOT-CA-1.cer -u admin  
-k ./GAAKprivatekey.pem key-get-wrapping-key -c KWK1.pem -t tokenKWK1 2048
```

Generating wrapping key with parameters:

key size: 2048

Wrapping key certificate written to: KWK1.pem

Token written to: tokenKWK1

3. Generate an operator secret.



For production environments, it is recommended to generate and store the operator secret in secure hardware. In the following example, we use standard OS tools and openssl to demonstrate the used algorithms.

The operator secret is used to protect the cHSM snapshots. Thus, having a backup copy of the operator secret is crucial.

In the example below, the file system of the host computer is used to generate a random value of 32 bytes. But it is recommended to use either a separate HSM or smartcard to do so and then encrypt the operator secret under the public part of the KWK.

Generate an operator secret:

```
dd if=/dev/urandom bs=32 count=1 of=OperatorSecret1

1+0 records in

1+0 records out

32 bytes copied, 0,000180998 s, 177 kB/s
```

For the Windows operating system, you can use `fileutils` to generate such random value.

4. Wrap the operator secret with the KWK (using the openssl command line tool).

```
openssl pkeyutl -encrypt -certin -inkey <Public_KWK> -pkeyopt
rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -pkeyopt
rsa_mgf1_md:sha256 -in <operator_secret_plain> -out
<wrapped_operatorsecret_under_KWK>
```

```
Example : openssl pkeyutl -encrypt -certin -inkey KWK1.pem -pkeyopt
rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -pkeyopt
rsa_mgf1_md:sha256 -in OperatorSecret1 -out OperatorSecret1_KWK1
```

5. Load the operator secret into the device.

Once the wrapped operator secret is ready, it can be loaded into the u.trust Anchor device via gladm.

```
gladm -d <device_IP> -u <username> -k <credentials> key-import-operator-
secret <token_name> <wrapped_operatorsecret_under_KWK>
```

```
Example : gladm -d 10.17.72.6 -u admin -k ./GAAKprivatekey.pem key-import-
operator-secret tokenKWK1 OperatorSecret1_KWK1
```

Importing operator secret with parameters:

token: tokenKWK1

secret: OperatorSecret1_KWK1

Fingerprint of imported Operator Secret: f5c009b1

6. Check that the operator secret has been loaded.

```
gladm -d <device_IP> -u <username> -k <credentials> key-list-operator-secrets
```

Example : `gladm -d 10.17.72.6 -u admin -k ./GAAKprivatekey.pem key-list-operator-secrets`

f5c009b1: 2022-01-14T19:09:26+0000 - active



The device is ready for snapshot and restore operations.

5.4 Copy an Operator Secret

This command allows a Global Administrator to copy an operator secret from smartcard to smartcard, or to transfer an operator secret from a key file to a smartcard. Therefore, the source of the secret may be a key file or a smartcard specifier, whereas the target must be a smartcard specifier.

Furthermore, the Global Administrator may specify the exact record number on the smartcard from and into which a key share shall be read or written, as well as the number of key shares.

If smartcards are used: A PIN pad including a smartcard reader can be connected to the computer where gladm is running (USB port) or to another computer. Watch the display of the PIN pad for instructions on further command processing.

If key files are used: We strongly recommend using encrypted key files. If encrypted key files are used, we strongly recommend using a hidden password entry.



Global Administrators should use a dedicated smartcard for operator secrets (and not use the same smartcard for MBKs, for example).

Procedure for copying from a smartcard to a smartcard:

1. Connect the smartcard reader to the device and insert the smartcard.

2. Perform the command `gladm smartcard-copy-secret`. The following example copies an operator secret from smartcard to smartcard, reading and writing from and into the default record number 7.

```
gladm smartcard-copy-secret :cs2:cjo:USB0 :cs2:cjo:USB0
```

3. The command is executed and a message on the smartcard reader will be displayed, prompting the user when to press **OK** and when to insert the next smartcard.
4. The copied operator secret share is stored in the target smartcard using the default record number 7.



Upon successful copying of the operator secret, a message that the operation has been successfully completed is displayed.

Procedure for copying from a key file to a smartcard:

1. Connect the smartcard reader to the device and insert a smartcard.
2. Perform the command `gladm smartcard-copy-secret`. The following example copies an operator secret, creates 2 out of 2 shares from a file and puts them on smartcards in record number 6.

```
gladm smartcard-copy-secret -t 6 -k 2 secret_key_file :cs2:cjo:USB0
```

3. The command is executed and a message on the smartcard reader will be displayed, prompting the user when to press **OK** and when to insert the next smartcard.
4. The copied operator secret shares are stored in the target smartcards using record number 6.



Upon successful copying of the operator secret, a message that the operation has been successfully completed is displayed.



An operator secret share stored on a smartcard cannot be deleted, it can only be overwritten. If another share is already stored in the specified record, it is overwritten by the share generated by using the override flag option. See the [u.trust Anchor FIPS 140-3 - Administration Manual](#) for details.



For more information on smartcard specifiers, please see the *Generating an Operator Secret* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

5.5 Managing the MBK on u.trust Anchor

The capability to manage the cHSM (snapshot, create, restore, clone, etc.) via gladm introduces alternatives for MBK management. It is possible to perform a full snapshot of the cHSM with the gladm interface, thus capturing the contents of the cHSM (including the MBK).

When the OPERATOR instantiates the cHSM, a default MBK is randomly generated in the cHSM. The cHSM TENANT can decide to generate their own MBK and load it to replace the default generated MBK, but can also decide to grant the OPERATOR the capability to perform the snapshot/restore/clone functions.

In the case that the CUSTOMER would like more cHSMs with the same MBK, the OPERATOR can simply snapshot and restore the cHSM, thus duplicating the cHSM with its content including the MBK.

Therefore, the cHSM TENANT is not required to manage the MBK backup and HSM snapshot and can delegate it to the OPERATOR, as desired.

Please note that the OPERATOR can only snapshot and restore the cHSM; the OPERATOR has no access to the keys. Only the cHSM TENANT with the cHSM Administrator keys can connect to the cHSM.

Taking a Snapshot

This command takes a snapshot of a cHSM and stores it so that it can be restored at a later point. For more information, see the *Taking a Snapshot (chsm-snapshot)* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

```
gladm -u <username> -k <credentials> -d <addr> chsm-snapshot -f  
snapshot_filename <slot_id>
```

Restoring a cHSM

This command restores a cHSM from a snapshot on a free slot. The snapshot is verified by the device operator secret before the cHSM is restored. The cHSM will be started in an operational state. For more information, see the *Restoring a cHSM (chsm-restore)* chapter in the [u.trust Anchor FIPS 140-3 - Administration Manual](#).

```
gladm -u <username> -k <credentials> -d <addr> chsm-restore -m <snapshot  
filename> <slot_id>
```

Retrieving a cHSM

This command sets the cHSM to a halted state, takes a snapshot, and retrieves it from the device. After the execution of this command, the cHSM will no longer be available on the device. The cHSM can still be restored or cloned using the snapshot. For more information, see the *Retrieving a cHSM (chsm-retrieve)* chapter in the [u.trust Anchor 140-3 - Administration Manual](#).

```
gladm -u <username> -k <credentials> -d <addr> chsm-retrieve [-f <val>] <slot  
id>
```

6 Contact Address for Support Queries

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m. Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

Other Support Queries

- Mail (preferred contact method)
support@utimaco.com
Attach the diagnostic information to your email.
- Web portal
<https://support.hsm.utimaco.com/support/cases/new/>
The diagnostic information will be requested in our response if necessary.
- By phone
AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301
The diagnostic information will be requested in our response if necessary.

7 References

<i>Reference</i>	<i>Title/Company</i>	<i>Document Number</i>
	u.trust Anchor FIPS 140-3 - Administration Manual / Utimaco IS GmbH	2023-0027
	u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (cHSM) - Administration Manual / Utimaco IS GmbH	2023-0028
	u.trust Anchor LAN V5 - Administration Manual / Utimaco IS GmbH	2023-0036