

CryptoServer LAN V5

Quick Start Guide



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	1.0.16
Product Version	6.0.0
Date	2024-10-24
Document No.	2018-0016
Status	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
2	Getting Started	5
2.1	Connect Power Supply and Switch on CryptoServer LAN.....	5
2.2	Change the root and cslagent Password	6
2.3	Open CryptoServer LAN Control Menu.....	7
2.4	Configure the IP Address (e.g., static IPv4).....	7
2.5	Set the IP Address for the Default Gateway	7
2.6	Enable the SSH Daemon.....	8
2.7	Preparation Steps (Admin Computer)	8
2.8	Connect the PIN Pad to the Administration Computer	8
2.9	Install the PIN Pad Driver	9
3	Initial Administration Steps	11
3.1	Connect to CryptoServer LAN (via CAT)	11
3.2	Configure the PIN Pad	11
3.3	Generate a New Smartcard Token	12
3.4	Change the Authentication Token for the Default User ADMIN	12
3.5	Log in to the CryptoServer as Default User ADMIN	14
3.6	Generate a Master Backup Key (MBK).....	14
4	Further Reading	16

1 Introduction

This document provides step-by-step instructions on how to bring the CryptoServer LAN into service, how to prepare a computer (Windows) for the CryptoServer administration and guides you through the initial administration steps. It does not cover all scenarios and 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 *CryptoServer LAN V5 Administration Manual* and the *CryptoServer Administration Manual*.

Before you start with the installation, read the safety instructions in the *CryptoServer LAN V5 Operating Manual* and examine the CryptoServer LAN device for obvious signs of damage.

2 Getting Started

2.1 Connect Power Supply and Switch on CryptoServer LAN



Front view



Dual power supply (AC)

eth0 eth1 VGA

CryptoServer PCIe card

Rear view

1. Connect the two independent 100 V - 240 V main power supplies.
2. Connect an RJ45 network cable to Ethernet port **eth0**.
3. Turn on the power switch.
The CryptoServer LAN is ready for operation after approx. 90 seconds.
4. The display shows alternating status information.

```
- CryptoServer LAN -
HSM Model:
  SecurityServer
  Se1500 CS132456
```

```
- CryptoServer LAN -
HSM Battery
Voltage:    3.045 V
           OK
```

```
- CryptoServer LAN -
Time (local/UTC)
2018-09-20 13:00:33
2018-09-20 12:00:33
```

```
- CryptoServer LAN -
HSM Status (1/2)
Mode:      Operational
Admin Mode: no
```

```
- CryptoServer LAN -
CSLAN Status
Connections: 2
Trans./min.: 7 TPM
```

```
- CryptoServer LAN -
Fan speed
F: 6100 6100 6200
B: 5300 5200 5200
```

```
- CryptoServer LAN -
HSM Status (2/2)
Temperature: 30.0 °C
Load:       0.0 %
```

```
- CryptoServer LAN -
CSLAN Battery
Voltage:    3.066 V
           OK
```

5. Make sure that the second display shows **Mode: Operational**.

2.2 Change the root and cslagent Password

1. Connect a monitor to the VGA connector on the rear side of CryptoServer LAN.
2. Connect a keyboard to the Host1 or Host2 USB port on the front panel of the CryptoServer LAN.
3. Log in to the the CryptoServer LAN as the user `root`.

```
CryptoServer login: root
Password: utimaco
```

4. Change the password of the user `root`:

```
root@CryptoServer:~# passwd
```

5. Enter the new password.

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

6. Log in to the the CryptoServer LAN as the user `cslagent`.

```
su - cslagent
```

7. Change the password of the user `cslagent`.

```
cslagent@CryptoServer:~# passwd
```

8. Enter the old password.
9. 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.
10. Log out from CryptoServer LAN with the `exit` command.
11. Perform the exit command once more.
12. Disconnect the monitor and the keyboard from CryptoServer LAN.

2.3 Open CryptoServer LAN Control Menu

Press **ENTER** to show the CryptoServer LAN menu on the display.

```
---- CSLAN menu -- ↓
CSLAN admin.
HSM admin.
PIN Pad applications
```

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

1. Select **CSLAN admin.** > **Configuration** > **Network IP4** by pressing the **ENTER** button.
2. Use the **↓** button to select **eth0** and press **ENTER** to open the menu item.
3. Use the **↓** button to select **Address** and press **ENTER** to open the menu item.
4. Enter the IP address by using the **↑→↓←** keys. Then press **ENTER**, the **→** key and **ENTER** again to confirm.

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

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

2.5 Set the IP Address for the Default Gateway

1. Select **CSLAN Admin.** > **Configuration** > **Network IP4** > **Default gateway** by pressing the **ENTER** button.
2. Enter the IP address by using the **↑→↓←** keys. Then press **ENTER**, the **→** key and **ENTER** again to confirm.

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

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

2.6 Enable the SSH Daemon

If the SSH daemon is disabled (default: enabled), enable it by performing the following steps:

Consider that CryptoServer LAN uses different SSH keys for each boot partition.

1. Select **CSLAN Admin.** > **Configuration** by pressing the **ENTER** button.
2. Use the **↓** button to select **Services** and press **ENTER** to open the menu item.
3. Press **ENTER** to select **SSH**.
4. Use the **↓** button to select **enabled** and press **ENTER** to open the menu item.
5. Use the **←** or **→** button to select **[*] Yes** and press **ENTER**.

2.7 Preparation Steps (Admin Computer)

1. 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.

2.8 Connect the PIN Pad to the Administration Computer

1. Connect the delivered PIN pad to a USB port of the administration computer.



Utimaco cyberJack one PIN pad

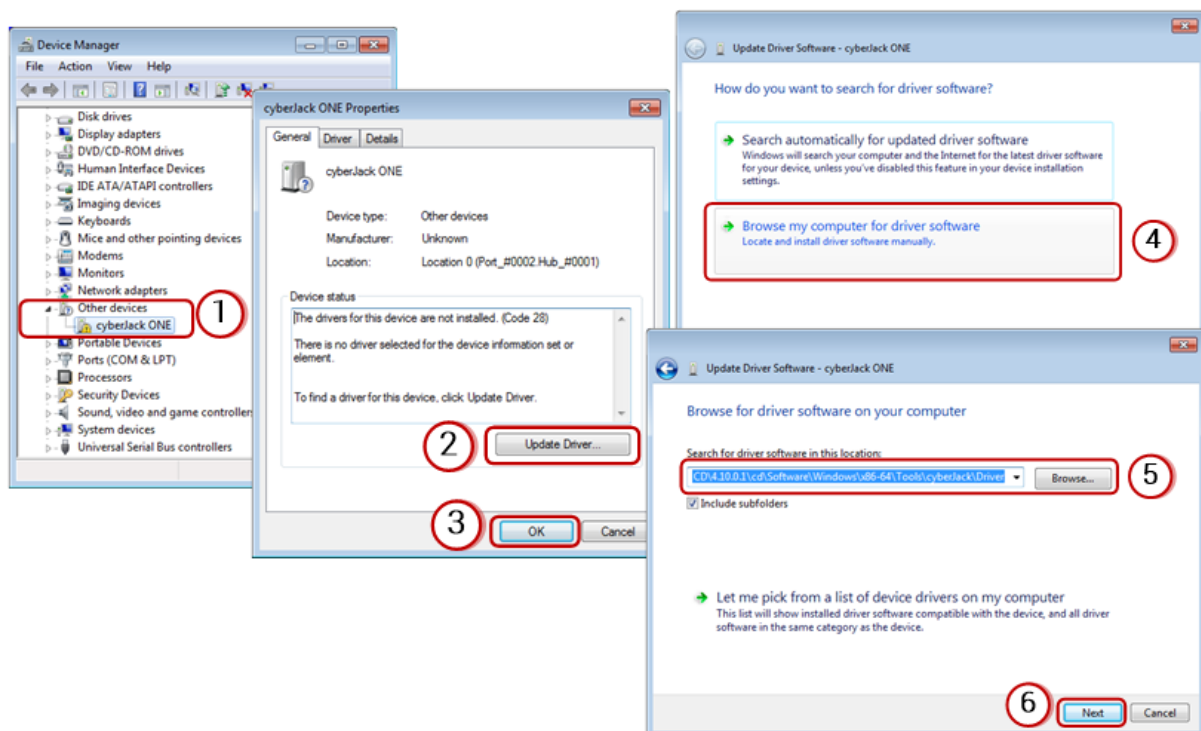
2. Install the PIN pad driver.

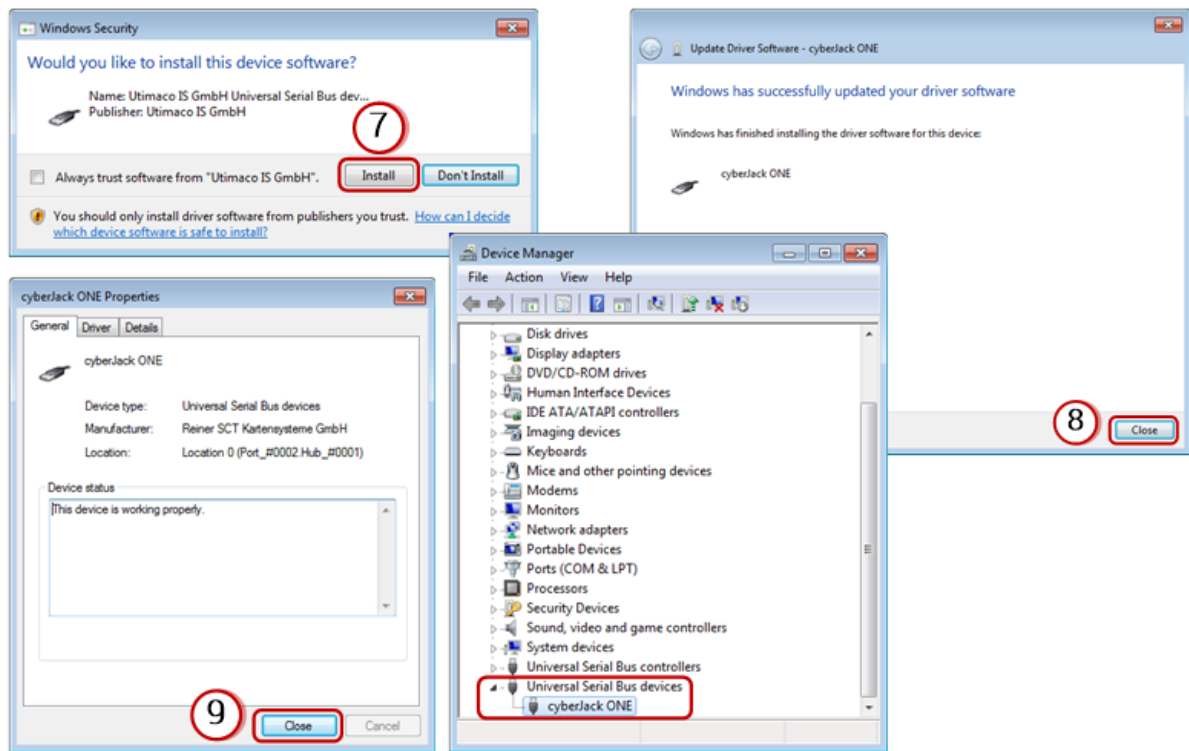
You find the corresponding files in the SecurityServer product bundle:

```
... \Software\Windows\Tools\cyberJack\Driver
```

2.9 Install the PIN Pad Driver

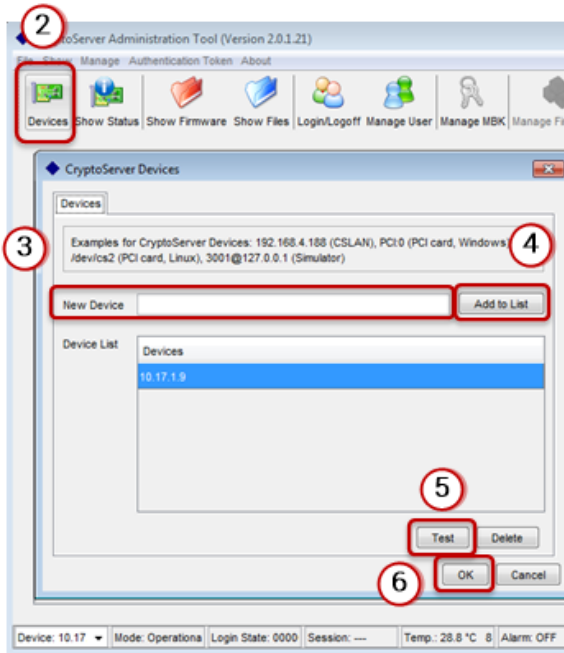
The example shows the installation of Utimaco's PIN pad driver for Utimaco cyberJack one on a Windows 7 computer.



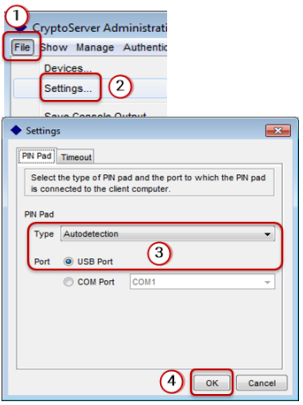


3 Initial Administration Steps

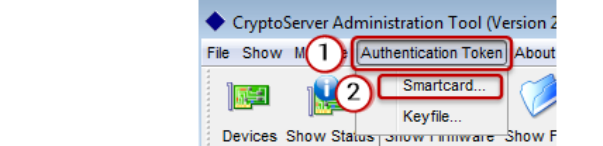
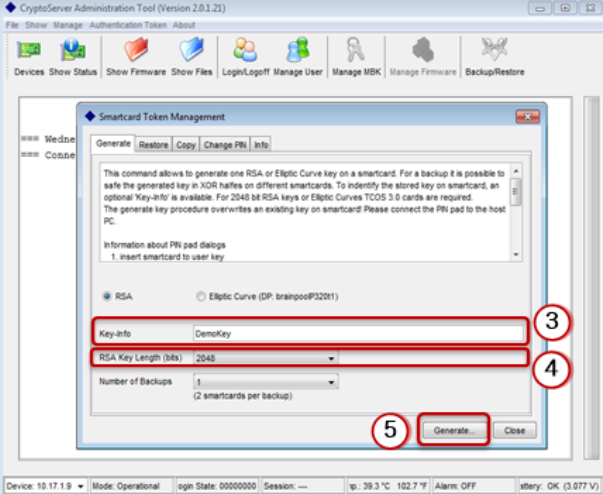
3.1 Connect to CryptoServer LAN (via CAT)

1	Install the SecurityServer package from the product bundle: SecurityServer-<version>.msi or CryptoServerSetup-<version>.exe CryptoServer Administration Tool (CAT) automatically starts after the installation.	
2	Click Devices in the CAT toolbar.	
3	Enter the IP address of the CryptoServer LAN into New Device .	
4	Click the Add to List button.	
5	Click the Test button to ensure CAT can connect to the CryptoServer LAN.	
6	Click the OK button to save the settings.	

3.2 Configure the PIN Pad

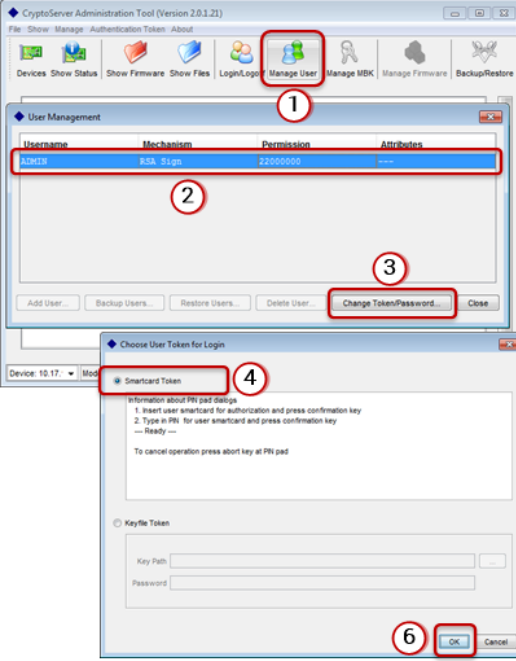
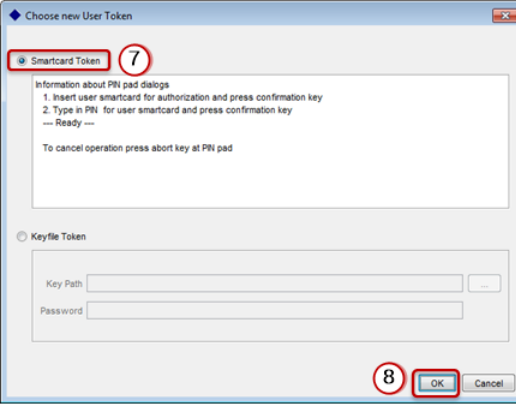
1	Click File in the CAT menu bar.	
2	Select Settings...	
3	Make sure Type is set to Autodetection and USB Port is selected.	
4	Click OK to save the settings.	

3.3 Generate a New Smartcard Token

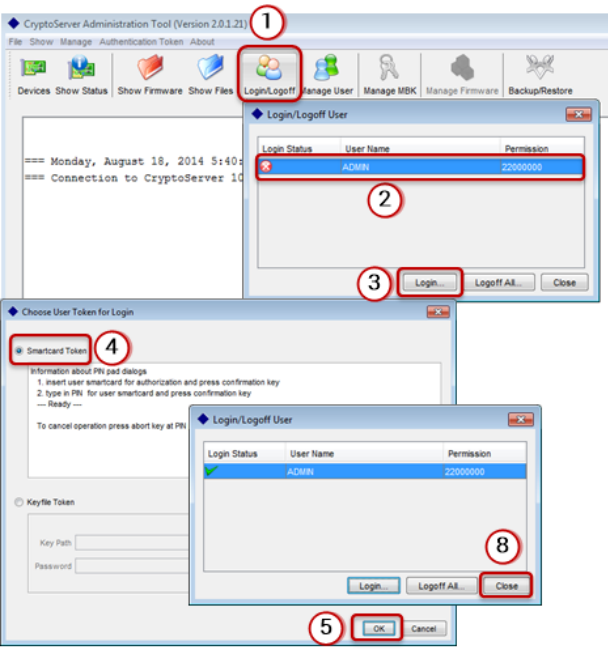
1 Click Authentication Token in the CAT menu bar.	
2 Select Smartcard...	
3 In the Key-Info text box, enter a key name.	
4 Select 2048 for RSA Key Length (bits) .	
5 Click Generate...	
6 Follow the instructions on the PIN pad. At first insert the smartcard for the authentication token. Next insert the 1st and 2nd smartcard for the authentication token backups. Default PIN: 123456	

3.4 Change the Authentication Token for the Default User ADMIN

Here the change is shown using smartcards.

1	Click Manage User in the CAT toolbar.	
2	Select the user ADMIN .	
3	Click Change Token/Password...	
4	Keep the Smartcard Token option selected and click OK to log in as ADMIN to the CryptoServer.	
5	Follow the instructions on the PIN pad. Use a smartcard with the old authentication token for the user ADMIN delivered by Utimaco (PIN: 123456) to authenticate the change. Use the OK button on the PIN pad for confirmation.	
6	Click OK to close the CAT login confirmation message.	
7	Keep the Smartcard Token option selected as the new authentication token for the user ADMIN.	
8	Click the OK button.	
9	Follow the instructions on the PIN pad. Use the smartcard with the previously generated smartcard token. A message appears to confirm the successful change of the authentication token for the user ADMIN.	

3.5 Log in to the CryptoServer as Default User ADMIN

1	Click Login/Logoff in the CAT toolbar.	
2	Select the ADMIN user.	
3	Click the Login... button.	
4	Keep Smartcard Token selected.	
5	Click the OK button.	
6	Insert the smartcard with the new authentication token into the PIN pad.	
7	Follow the instructions on the PIN pad.	
8	Click the Close button.	

3.6 Generate a Master Backup Key (MBK)

An MBK is a 256-bit AES key used for backup, encryption of external key storage or synchronization of CryptoServer in a cluster.

Keep three smartcards, delivered by Utimaco, at hand.

1	Click Manage MBK in the CAT toolbar.	
2	Enter an MBK Name .	
3	Keep m out of n selected.	
4	Keep m (Shares) = 2 and n (Shares) = 3 selected	
5	Select Automatic MBK Import .	
6	Click Generate...	
7	Select MBK Smartcard Token .	
8	Click OK .	
9	Enter the first MBK smartcard into the PIN pad.	
10	Press OK on the PIN pad.	
11	Enter the smartcard PIN and press OK on the PIN pad.	
12	Close the confirmation message for the creation of the first MBK share with OK .	
13	Repeat steps 7 to 12 for the other two MBK shares/MBK smartcards.	
14	Close the confirmation message for the creation of all MBK shares with OK .	
15	Select the Info tab to see all details about the MBK stored in the CryptoServer.	
16	Click CardInfo to show details about the MBK share stored on the smartcard currently inserted in the PIN pad, and press OK on the PIN pad.	

4 Further Reading

After you have finished performing the steps described in this document, your CryptoServer LAN is prepared to be fully integrated into your system infrastructure and to get operational.

Please find detailed information on the full range of setup and configuration options, as well as information about possible integration scenarios in the SecurityServer product bundle in the [Documentation](#) directory. Recommendations for further reading:

CryptoServer LAN V5 Administration Manual

CryptoServer Administration Manual

CryptoServer csadm Manual

CryptoServer CAT Manual

CryptoServer LAN V5 Operating Manual