



CryptoServer LAN

Quick Start Guide

Version 1.2.1

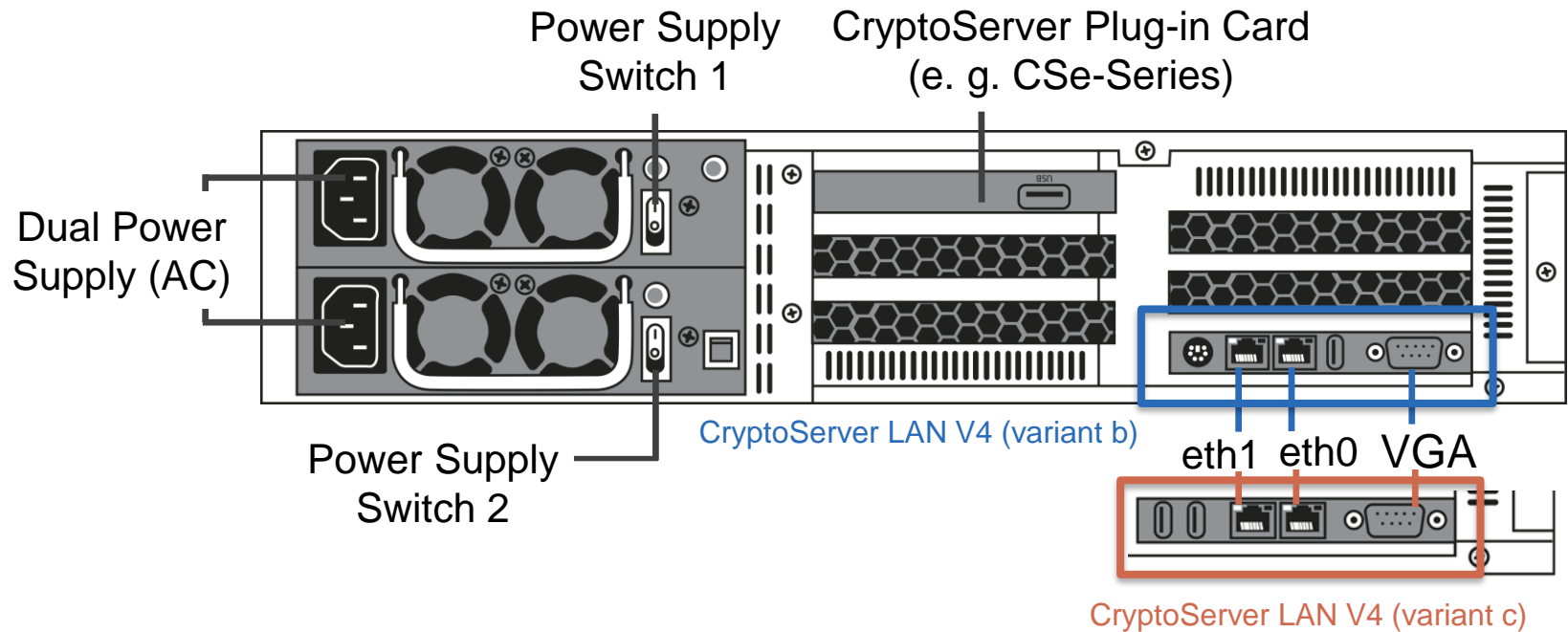
utimaco[®]

This document provides step-by-step instructions on how to bring the CryptoServer LAN into service, how to prepare a computer (Windows 7) for the CryptoServer administration and guides you through the initial administration steps. It doesn't cover all scenarios and is intended as a supplement to the documentation provided on the delivered product CD.

For detailed information on the full range of setup and configuration options, please read the [CryptoServer LAN Manual for System Administrators](#) and the [CryptoServer Manual for System Administrators](#).

Before you start with the installation, read the safety instructions in the [CryptoServer LAN V4 Operating Manual](#) and examine the CryptoServer LAN device for obvious signs of damage.

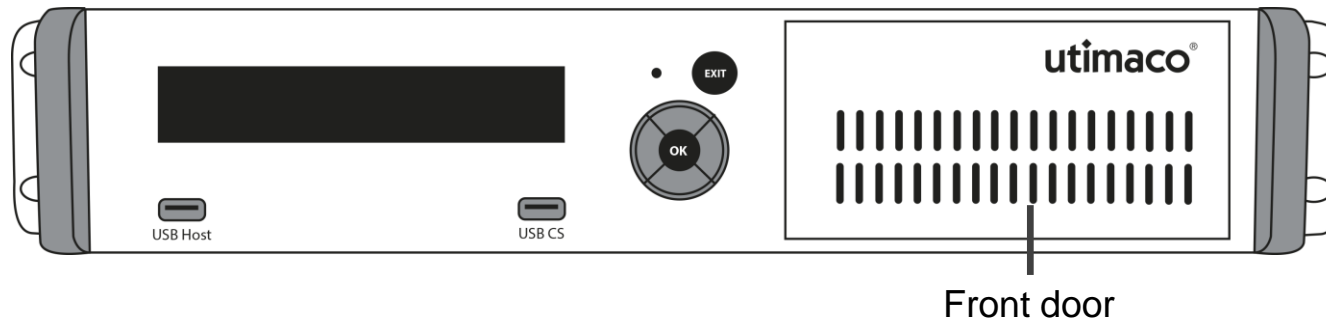
Connect Power Supply and Network



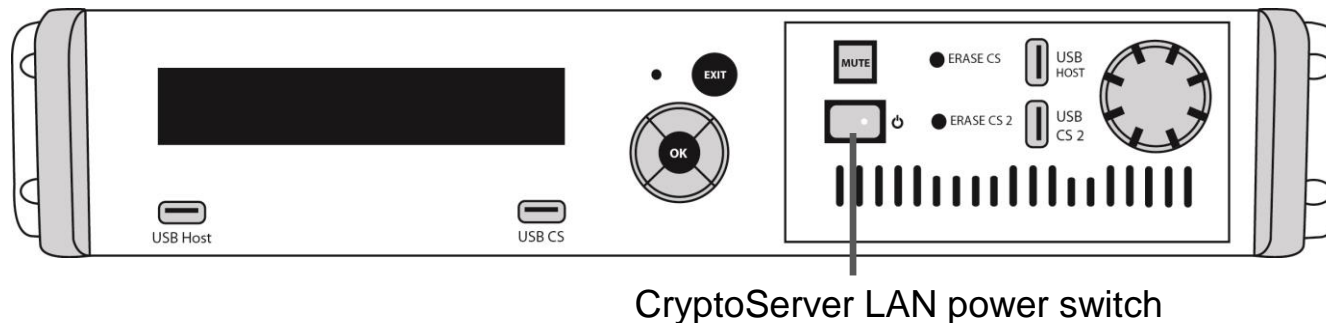
1. Connect two independent 100-240 V mains power supplies.
2. Connect an RJ45 network cable to Ethernet port **eth0**.
3. Turn on both power supply switches.

Switch on the CryptoServer LAN

1. Open the front door of CryptoServer LAN.



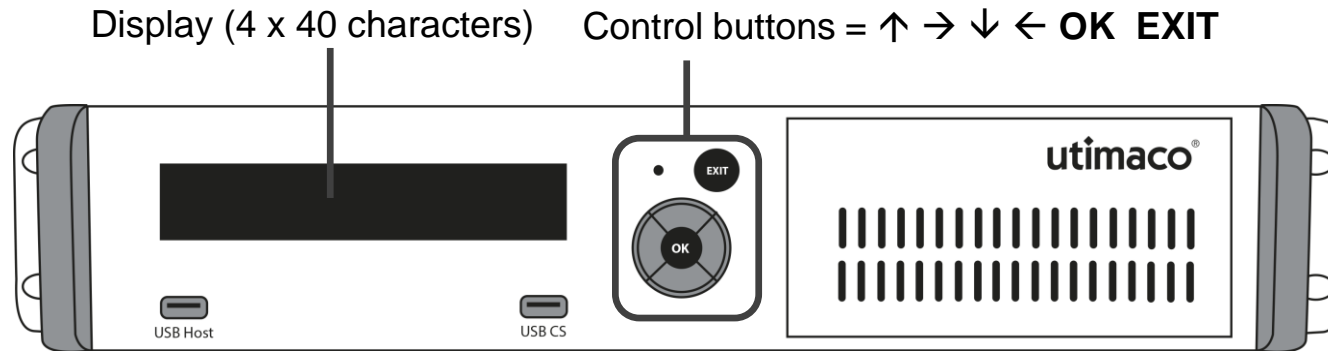
2. Press the CryptoServer LAN power switch.
CryptoServer LAN is ready for operation after approx. 30 seconds.



Change the root Password

1. Connect a monitor to the VGA connector on the rear side of CryptoServer LAN.
2. Connect a keyboard to the **USB Host** port on the front panel of the CryptoServer LAN.
3. Logon 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.
6. Log out from CryptoServer LAN with the `exit` command.
7. Disconnect the monitor and the keyboard from CryptoServer LAN.

Open CryptoServer LAN Control Menu



1. Make sure the display shows **Mode: Operational**, e. g.:


```
CryptoServer Se
Mode: Operational  OK  Temp.: 31,3 °C
Trans./min.:      0   Clients: 2
Load:             0 %
```

2. Press **OK** to show the CryptoServer LAN menu on the display.

```
[/
→ CSLAN Administration →
CryptoServer Administration →
PIN Pad Applications
```

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

1. Select **CSLAN Administration > Configuration > Network > IP Address** by pressing the **OK** button.
2. Press **OK** to select **IPv4 Address**.
3. Press **OK** to select **network interface: eth0**.
4. Enter the IP address by using the **↑ → ↓ ←** keys.

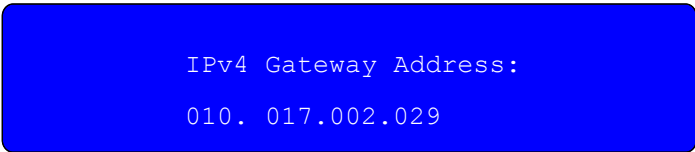


```
IPv4 Address:  
010. 017.002.009/18
```

↑ , ↓ = change the displayed digit
← , → = change the cursor position

Set the IP Address for the Default Gateway

1. Select **CSLAN Administration > Configuration > Network** by pressing the **OK** button.
2. Press the ↓ button to select **Default Gateway**.
3. Press **OK** to select **Default Gateway IPv4**.
4. Enter the IP address by using the ↑ → ↓ ← button.



IPv4 Gateway Address:
010. 017.002.029

↑ , ↓ = change the displayed digit
← , → = change the cursor position

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.

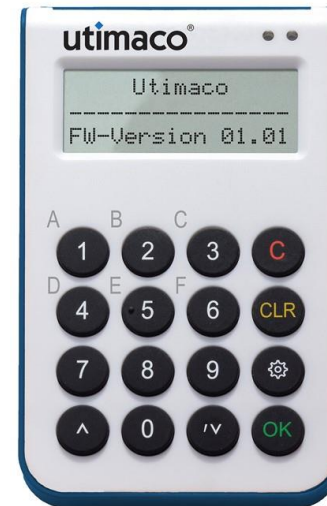
Connect the PIN Pad to the Admin Computer

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



REINERSCT cyberJack

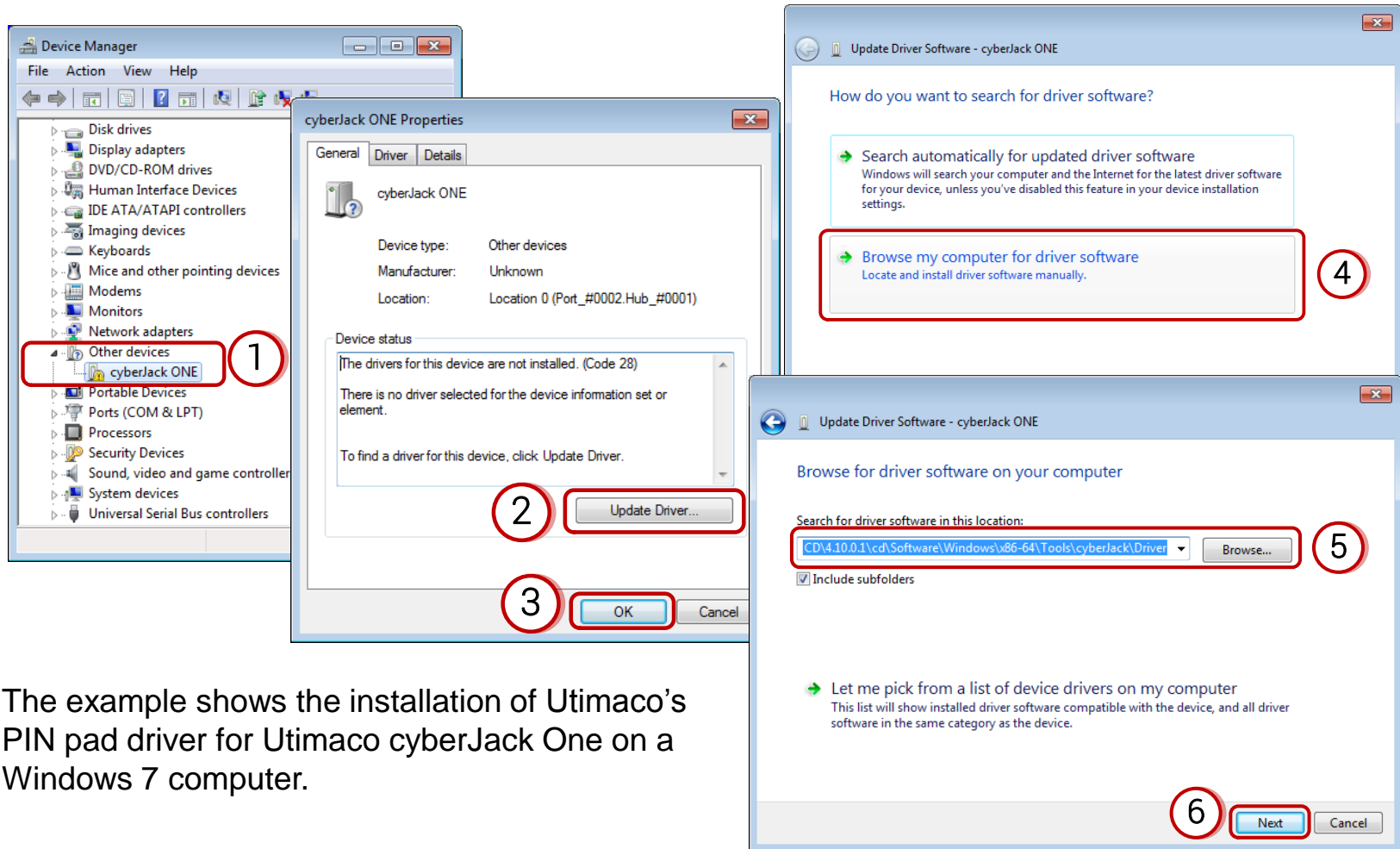
or



Utimaco cyberJack One

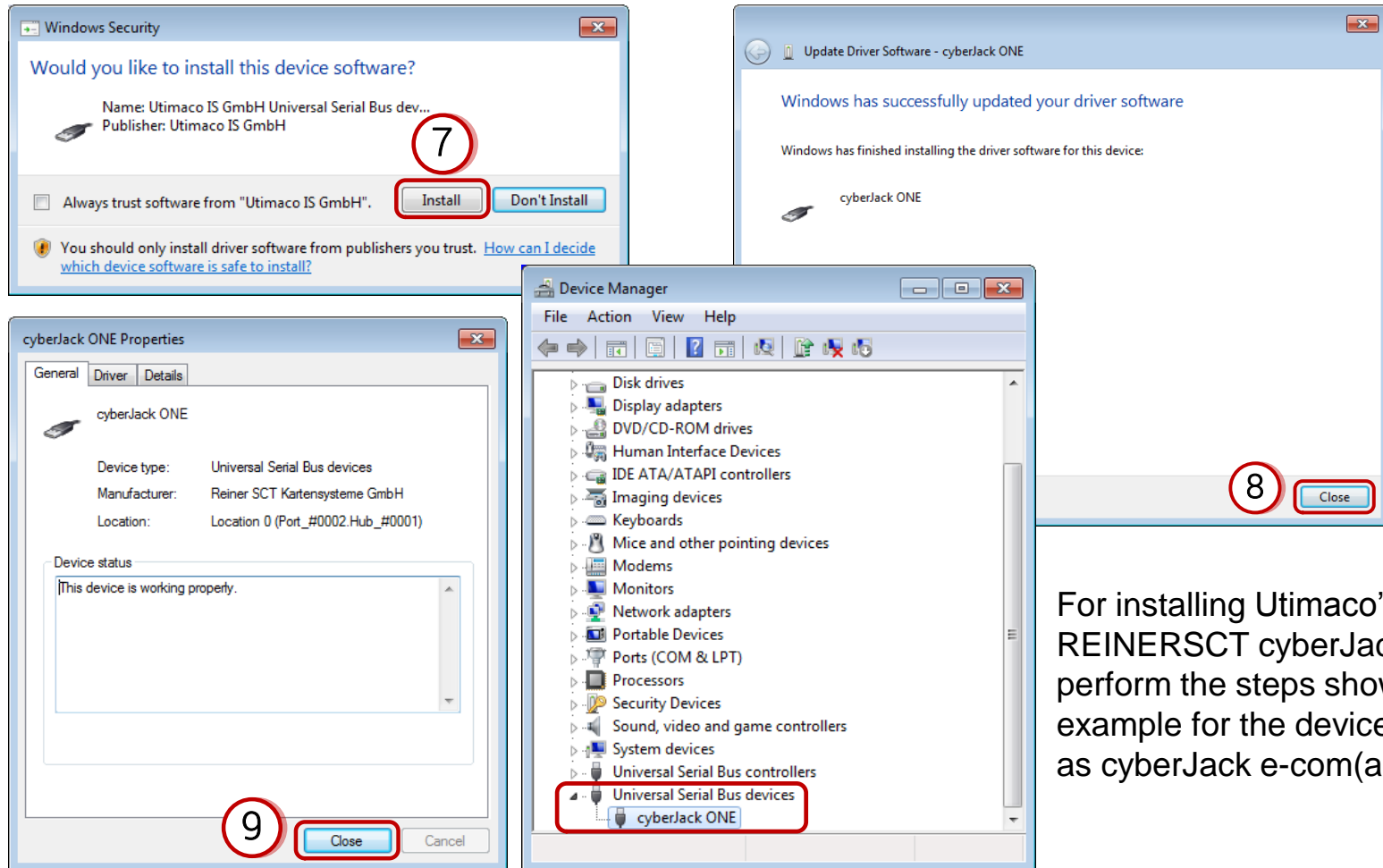
2. Install the PIN pad driver from the SecurityServer product CD:
 - 64-bit system ...\\Software\\Windows\\x86-64\\Tools\\cyberJack\\Driver
 - 32-bit system ...\\Software\\Windows\\x86-32\\Tools\\cyberJack\\Driver

Install the PIN Pad Driver 1/2



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

Install the PIN Pad Driver 2/2

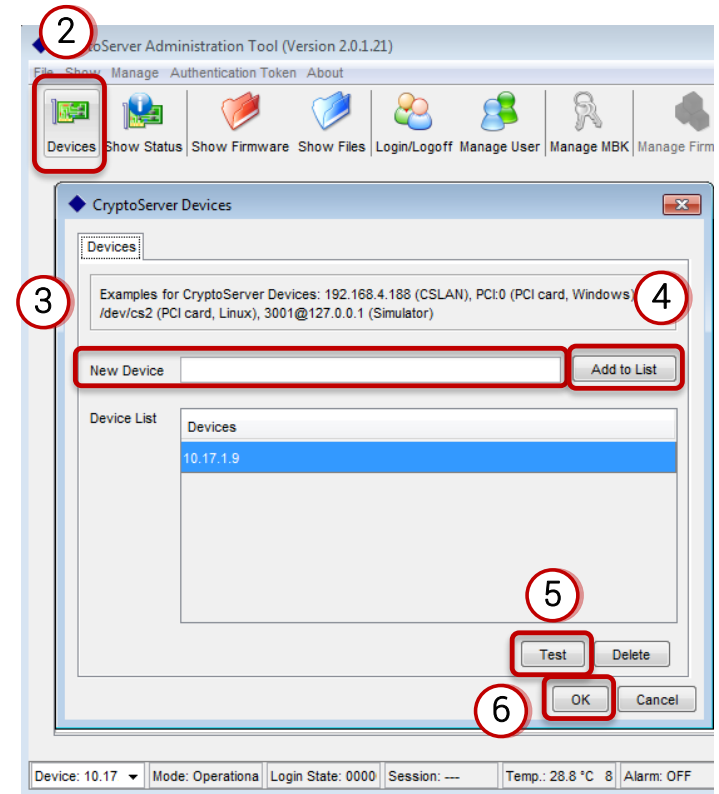


For installing Utimaco's driver for REINERSCT cyberJack PIN pad, perform the steps shown in this example for the device displayed as cyberJack e-com(a).

Initial Administration Steps

Connect to CryptoServer LAN (via CAT)

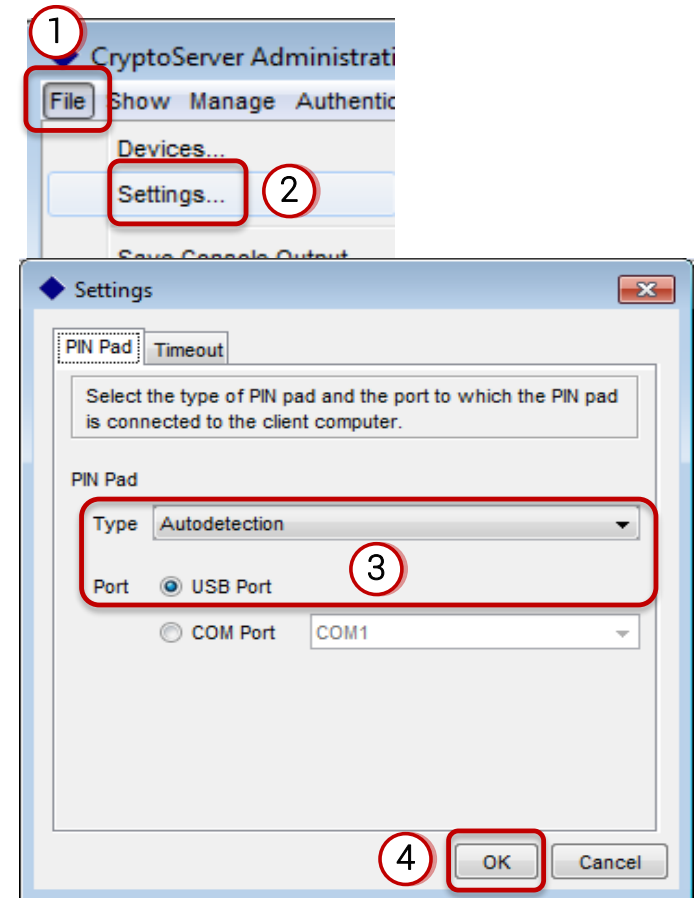
1. Install the SecurityServer package from the product CD:
CryptoServerSetup-<version>.exe
CryptoServer Administration Tool (CAT)
automatically starts after the installation.
2. Click **Devices** in the CAT toolbar.
3. Enter the IP address of the CryptoServer LAN into **New Device**.
4. Click the **Add 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.



Initial Administration Steps

Configure the PIN Pad

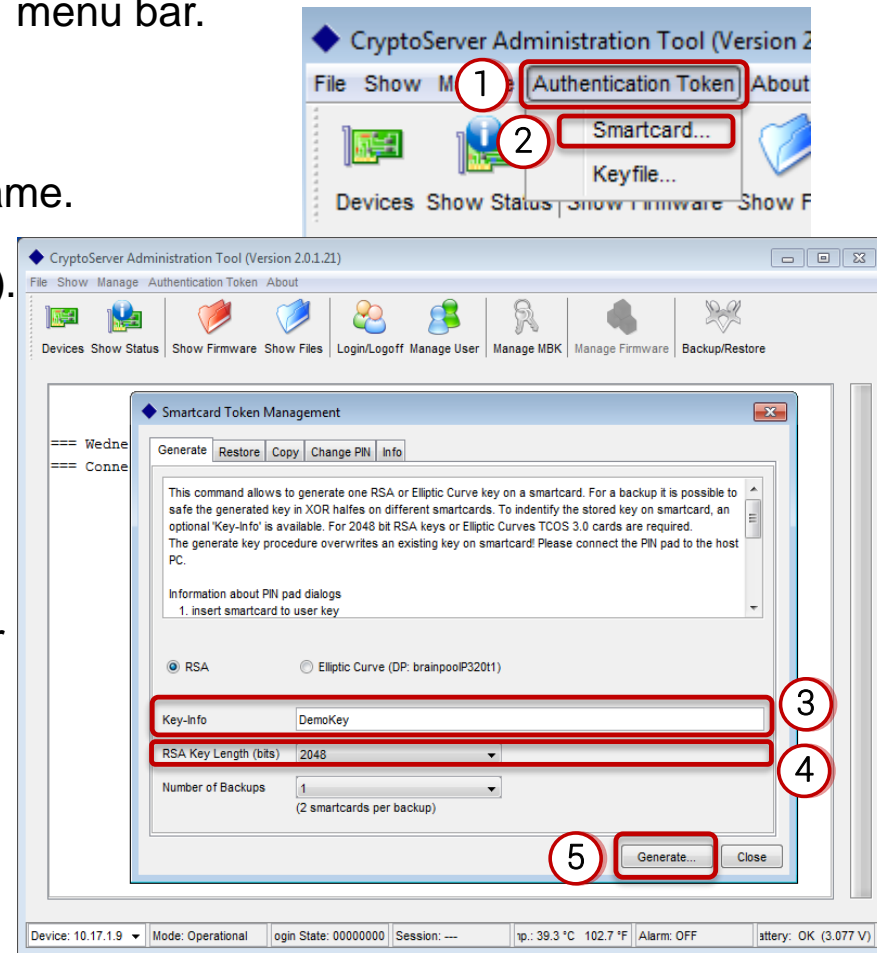
1. Click **File** in the CAT menu bar.
2. Select **Settings....**
3. Make sure **Type** is set to **Autodetection** and **USB Port** is selected.
4. Click **OK** to save the settings.



Initial Administration Steps

Generate a New Smartcard Token

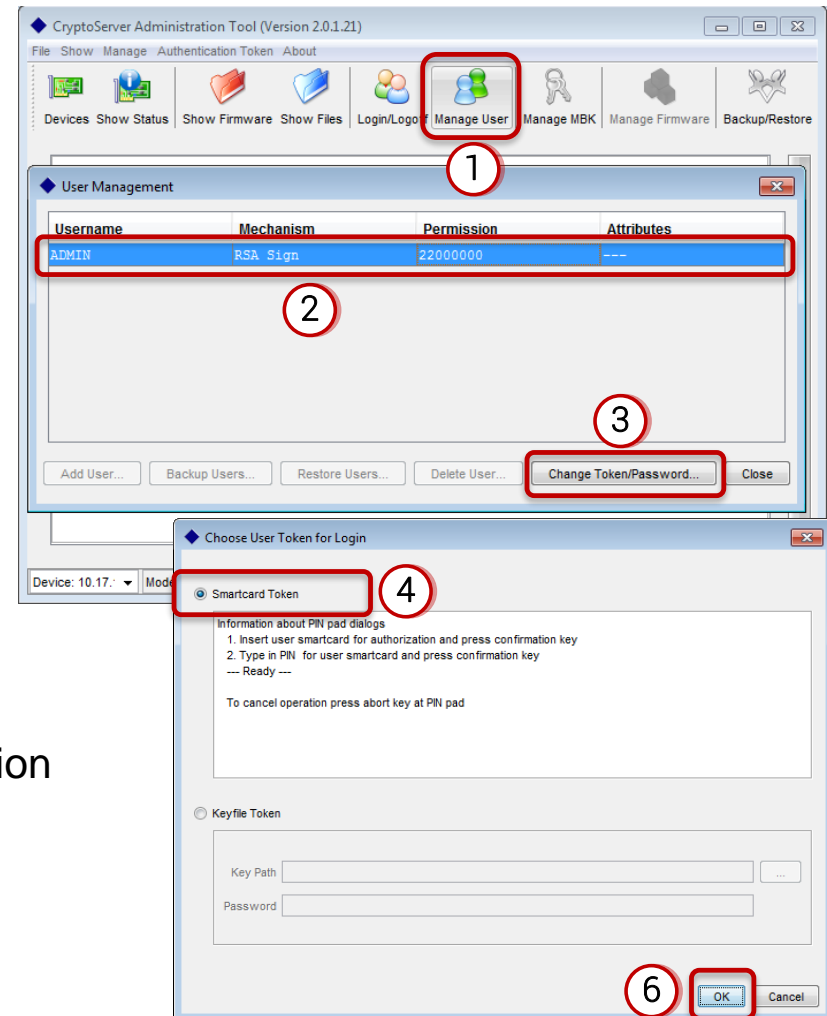
1. Click **Authentication Token** in the CAT menu bar.
2. Select **Smartcard...**
3. In the **Key-Info** text box, enter a key name.
4. Select **2048** for **RSA Key Length (bits)**.
5. Click **Generate...**
6. Follow the instructions on the PIN pad.
At first insert the smartcard for the authentication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



Initial Administration Steps

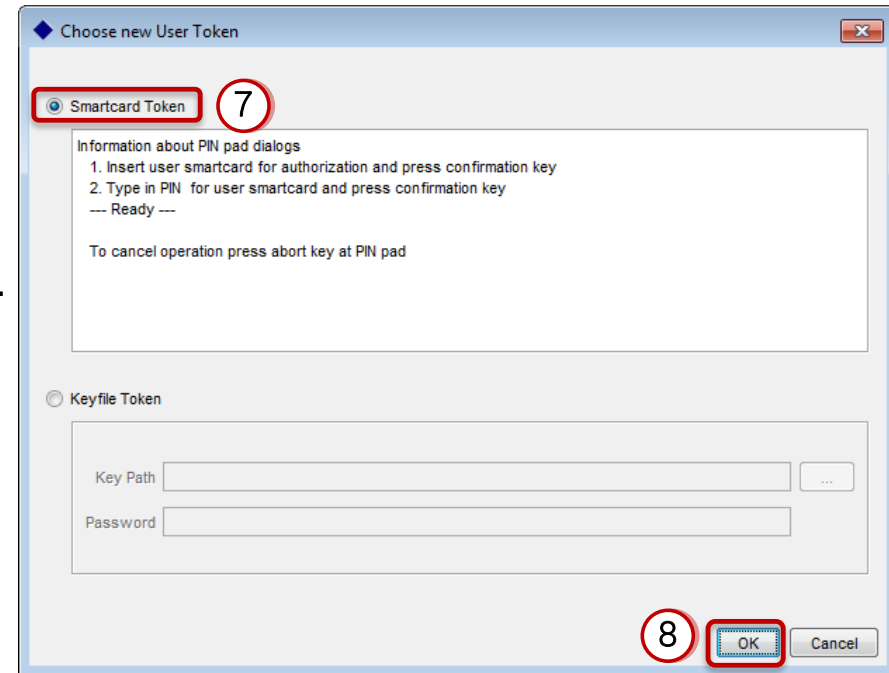
Change the Authentication Token for the Default User ADMIN (1/2)

1. Click **Manage User** in the CAT toolbar.
2. Select the user ADMIN.
3. Click **Change Token/Password...**
4. Keep **Smartcard Token** selected and click **OK** to logon as ADMIN to the CryptoServer.
5. Follow the instructions on the PIN pad. Use a smartcard delivered by Utimaco (PIN = 123456). Use the **OK** button on the PIN pad for confirmation.
6. Click **OK** to close the CAT login confirmation message.



Change the Authentication Token for the Default User ADMIN (2/2)

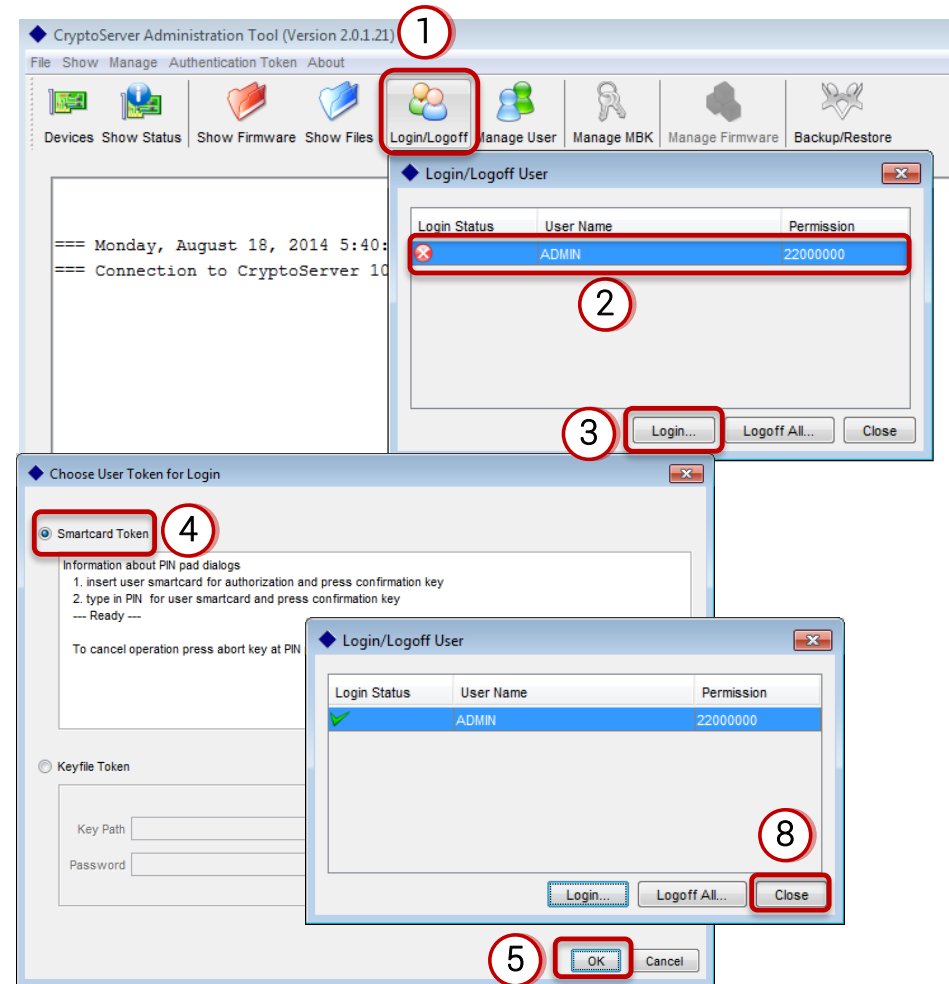
7. Keep **Smartcard Token** selected as the new authentication token for the user ADMIN.
8. Click the **OK** button.
9. Follow the instructions on the PIN pad. Use the smartcard with the previously generated smartcard token. A message appears to confirm the successful change of the authentication token for the user ADMIN.



Initial Administration Steps

Logon 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 auth. token into the PIN pad.
7. Follow the instructions on the PIN pad.
8. Click the **Close** button.



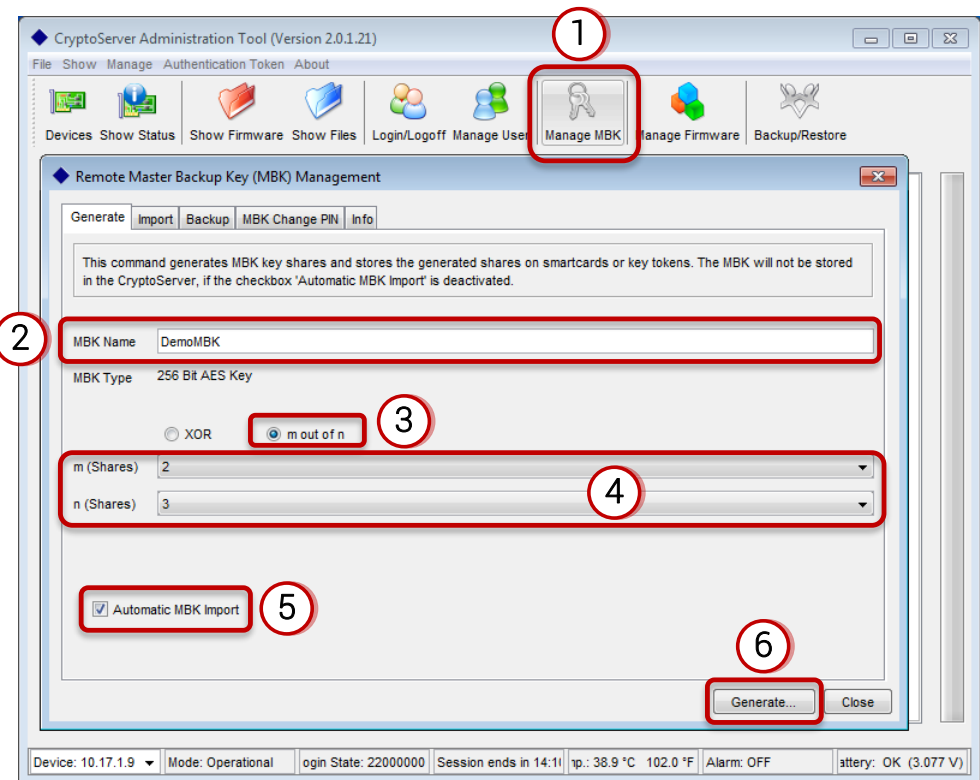
Initial Administration Steps

Generate a Master Backup Key (MBK) 1/3

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.

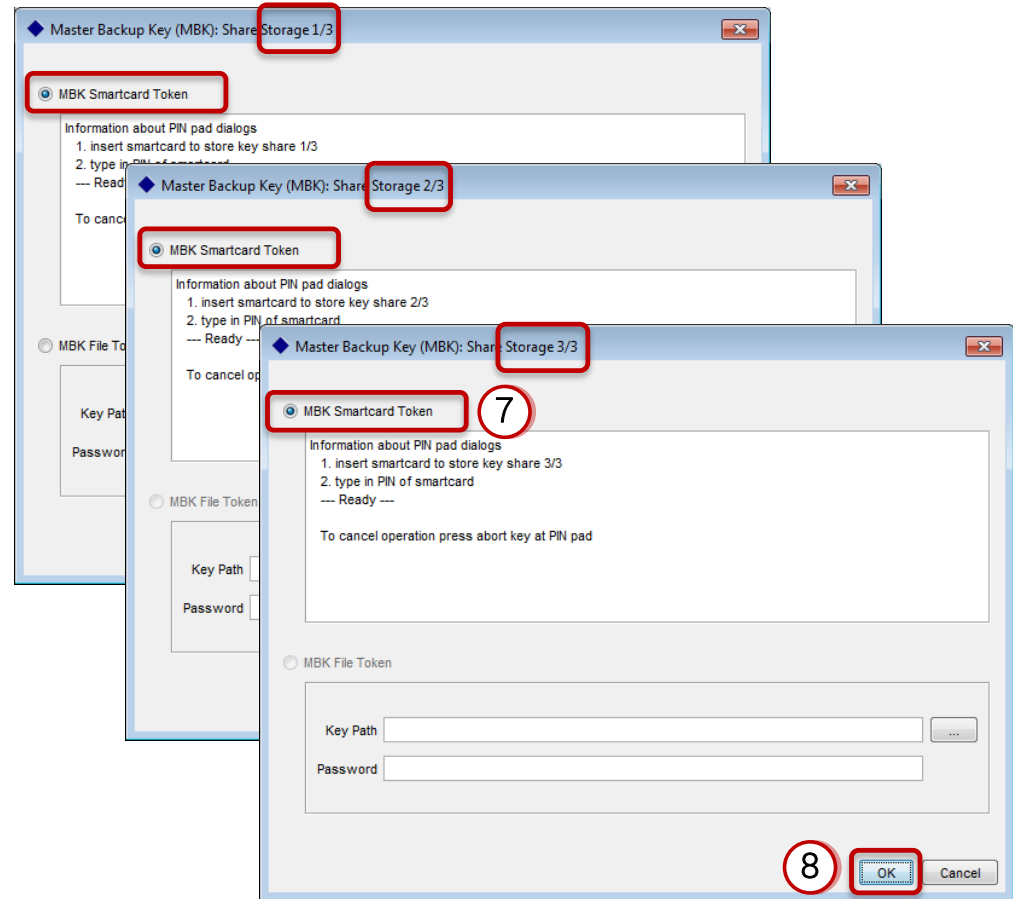
1. Click **Manage MBK** in the CAT toolbar.
2. Enter an **MBK Name**.
3. Keep **m out of n** selected.
4. Keep **m (Shares) = 2** and **n (Shares) = 3** selected.
5. Select **Automatic MBK Import**.
6. Click **Generate**....



Initial Administration Steps

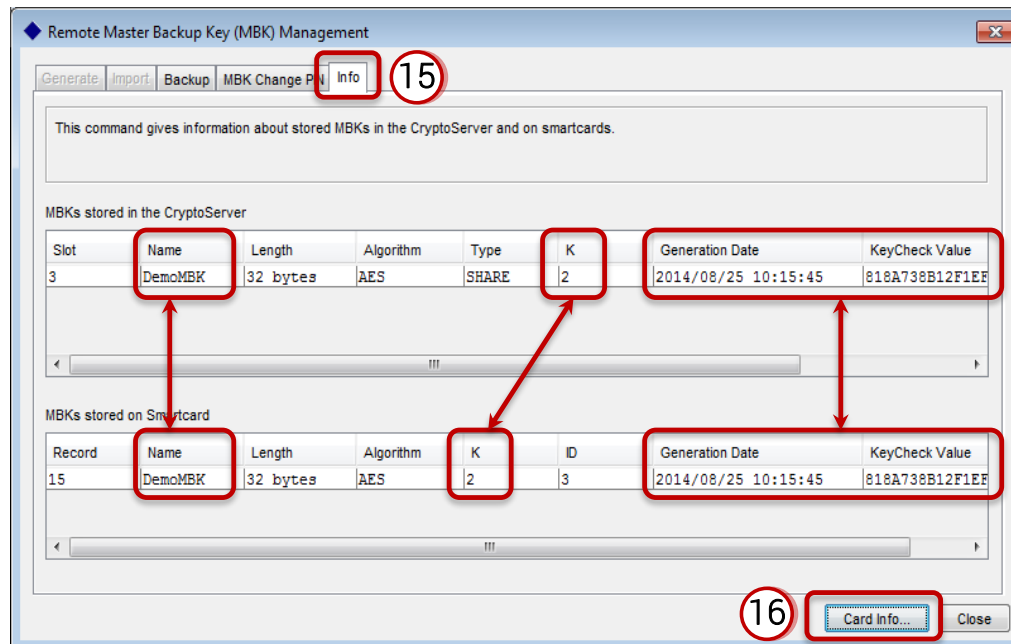
Generate a Master Backup Key (MBK) 2/3

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**.



Generate a Master Backup Key (MBK) 3/3

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.



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 on the SecurityServer product CD in the `Documentation` directory.

Recommendations for further reading:

[CryptoServer LAN Manual for System Administrators](#)

[CryptoServer Manual for System Administrators](#)

[CryptoServer csadm Manual for System Administrators](#)

[CryptoServer LAN V4 Operating Manual](#)



Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Germany

Tel.: +49 241 1696 200

Fax: +49 241 1696 199

E-mail: hsm@utimaco.com

Document number: M014-0001-en

Copyright © 2017 – Utimaco IS GmbH

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.

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.

All trademarks and registered trademarks are the property of their respective owners.