Delinea

Secret Server

Integration Guide

GP HSM Se-Series

utimaco®

Imprint

Copyright 2020	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	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	06/10/2025
Status	**PUBLISHED**
Document No.	IG-2025-0020

Table of Contents

1 Integrating Utimaco u.trust General Purpose HSM Se-Series with Secret Server

Third-party vendors create and maintain this integration. Delinea does not guarantee that the integration will work properly or that it respects Delinea product limitations. Delinea has not reviewed this integration and Delinea Support staff can only assist with the Delinea side of setup.

By integrating Delinea Secret Server with Utimaco u.trust General Purpose HSM Se-Series, organizations can benefit from both best-in-class privileged access management and advanced hardware security, safeguarding their most sensitive assets. This combined solution strengthens security, reduces risks, enhances compliance, and streamlines operations, offering robust, scalable protection across industries.

2 About Utimaco

Utimaco's u.trust General Purpose HSM Se-Series is engineered to meet stringent security standards and compliance requirements. It combines scalable multi-tenancy functionality with superior performance, making it a versatile solution for a wide range of applications. The HSM's container-based architecture supports up to 31 containers, offering flexibility for various use cases, including Post-Quantum Cryptography (PQC), 5G, blockchain, and custom applications.

Key Features of Utimaco u.trust General Purpose HSM Se-Series:

Performance of up to 40,000 RSA 2K operations per second: The u.trust General Purpose HSM SeSeries is available in multiple models, from entry-level to high-performance use cases.

Multi-tenancy for High Availability, Scalability, and Flexibility: The u.trust General Purpose HSM SeSeries offers scalable multi-tenancy and superior performance. Its container-based architecture supports up to 31 containers, enabling flexibility across use cases such as PQC (Post-Quantum Cryptography), 5G, blockchain, and custom applications.

Key Partitioning System:The system supports multiple PKCS #11 partitions per container to ensure application isolation and key separation.

Crypto-agile and PQC-ready: Designed for crypto-agility, with the ability to upgrade in-field with PQC algorithms such as ML-KEM, ML-DSA, LMS, HSS, XMSS, and XMSS-MT.

FIPS-certified up to 140-2 Level 3: The u.trust platforms are certified up to FIPS 140-2 Level 3 and can be optionally operated in FIPS mode.

Flexible Key Storage:The u.trust platforms support both internal and external key storage. You can also use a free simulator to test development and integration in your environment.

For more details on the u.trust General Purpose HSM Se-Series, go here.

The following Utimaco integration is available:

"Integrating Utimaco u.trust General Purpose HSM Se-Series with Secret Server" below

3 Configuring HSM in Utimaco

Configuring a Utimaco Hardware Security Module (HSM) involves several steps, including setting up the hardware, initializing the HSM, creating users, managing cryptographic keys, and ensuring the necessary software environment is in place.

3.1 Hardware Setup

Configuring a Utimaco Hardware Security Module (HSM) involves several steps, including setting up the hardware, initializing the HSM, creating users, managing cryptographic keys, and ensuring the necessary software environment is in place.

Hardware Setup

- Ensure you have all the necessary components (the HSM device, cables, etc.) that came with the Utimaco HSM.
- Connect the device to both a power supply and your network using the appropriate ports. This may include Ethernet cables for network access and power cables for the device itself.

Network Configuration

Set a Static IP Address:

- When you connect the HSM to your network, you must assign a static IP address so that it can be reliably accessed at all times.
- Access the HSM's network settings either through a management interface or command-line tool.
- Set:
    - Static IP address
    - Subnet mask (the range of IP addresses within your local network)
    - Gateway (the router or device that connects your network to the internet)
    - DNS servers (used for resolving domain names if required)

Installing Software Requirements

Install Java (LTS Version):

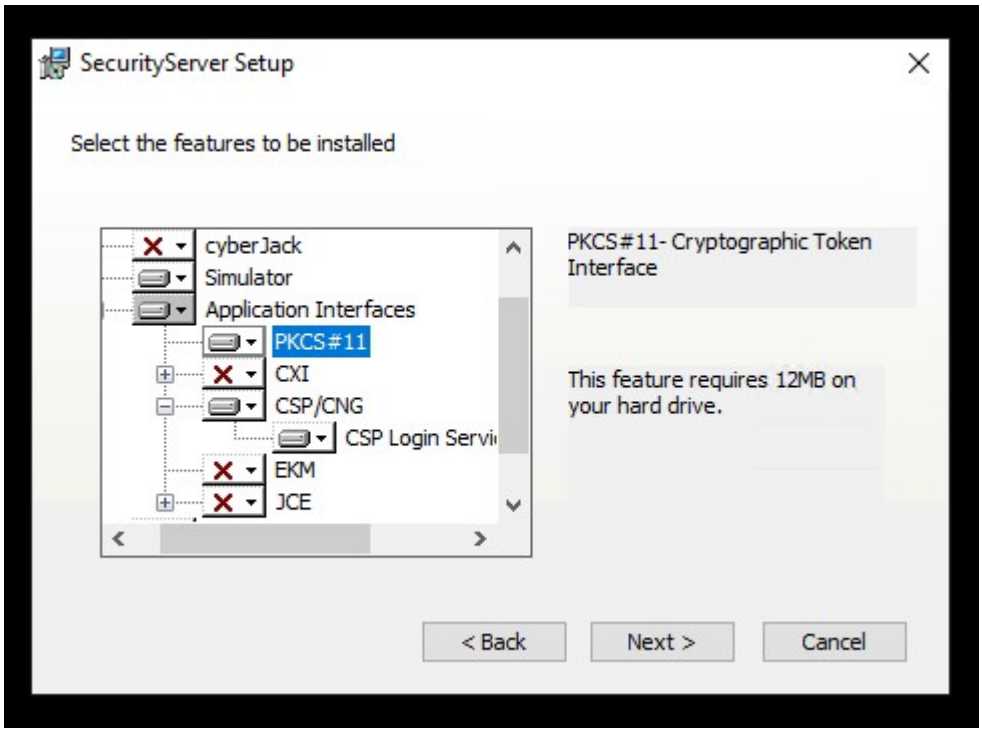
Download and install the latest Java LTS version, which is required to run the CryptoServer software.

Installing the Security Server:

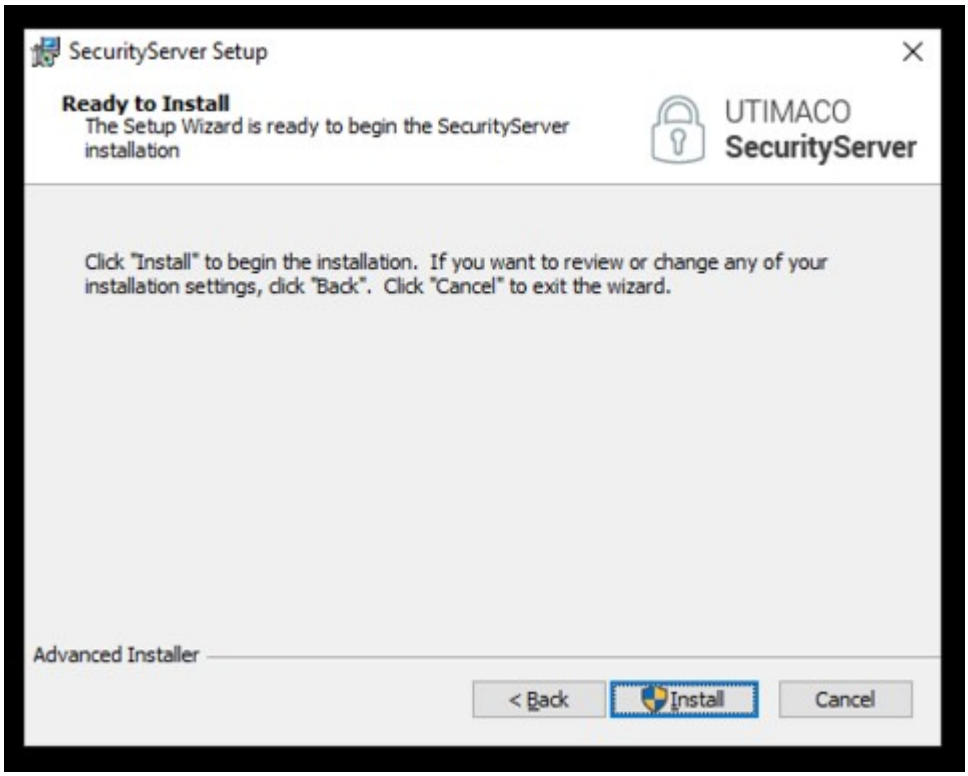
- Download SecurityServerEvaluation-V6.0.0.0.zip.

This software package will be provided by Utimaco.

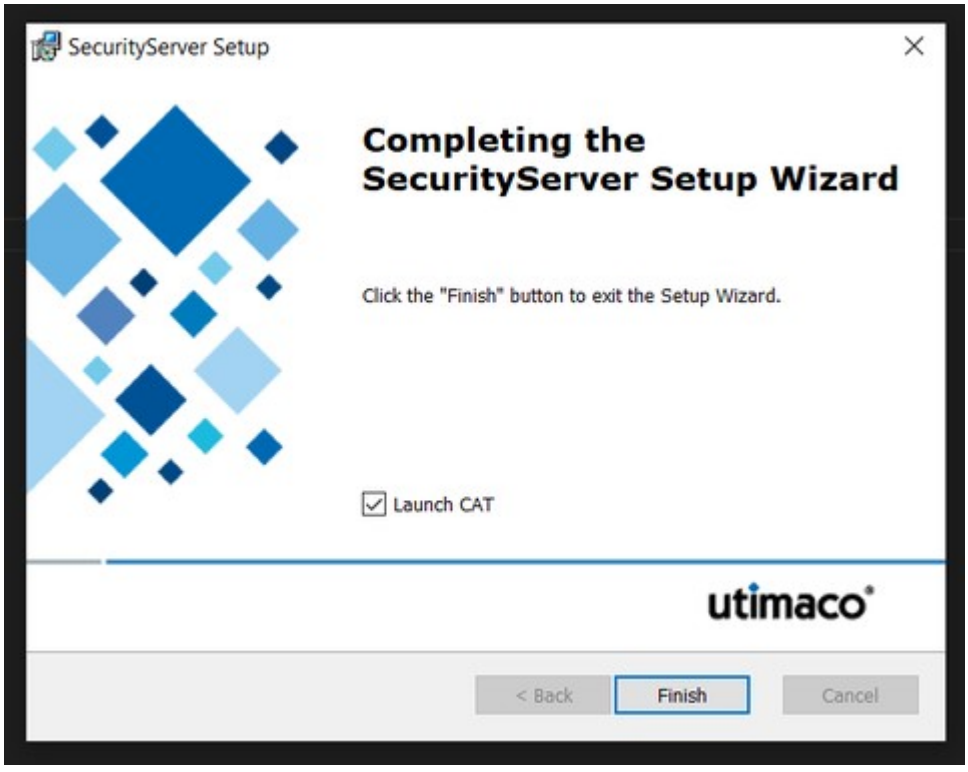
- Unzip the package and run SecurityServer-6.0.0.0.msi.
- Installation steps:
  - Choose the default folder(s) and select **Custom installation**.
  - Ensure the correct features are selected:
    - For PKCS#11, select the PKCS#11 feature.
    - For CNG, select the CSP/CNG feature.
- Select **Next**.



- Select **Install**.



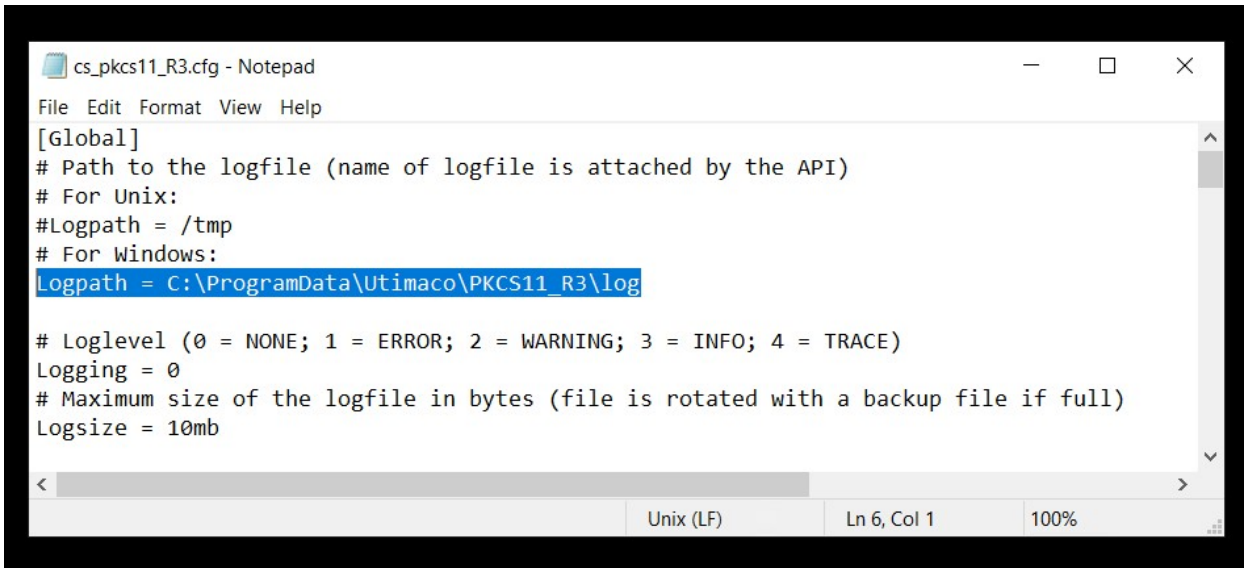
- Select **Finish**.



3.2 Setting up PKCS#11 / CNG

PKCS#11 Setup n Set up PKCS#11 files and log folders:

1. Navigate to **C:\ProgramData\Utimaco\PKCS11_R3** and create a **log** folder.
2. Update the **#Logpath = C:\ProgramData\Utimaco\PKCS11_R3** to **Logpath = C:\ProgramData\Utimaco\PKCS11_R3\log** inside the **cs_pkcs11_R3.cfg** file.



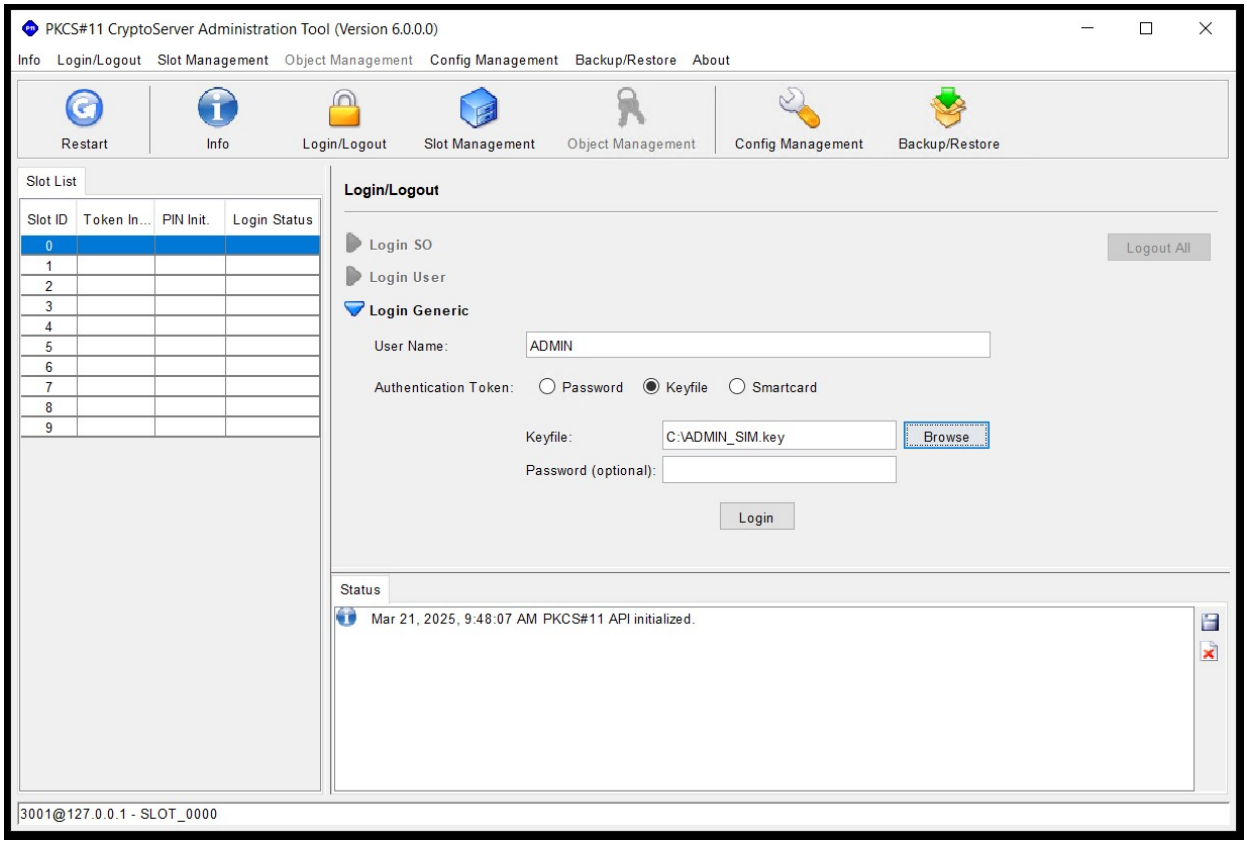
Initialize Slot Token and Set Up Users:

1. Open the PKCS#11 CryptoServer Administration Tool (CAT) by selecting the PKCS#11 icon on your desktop.

or

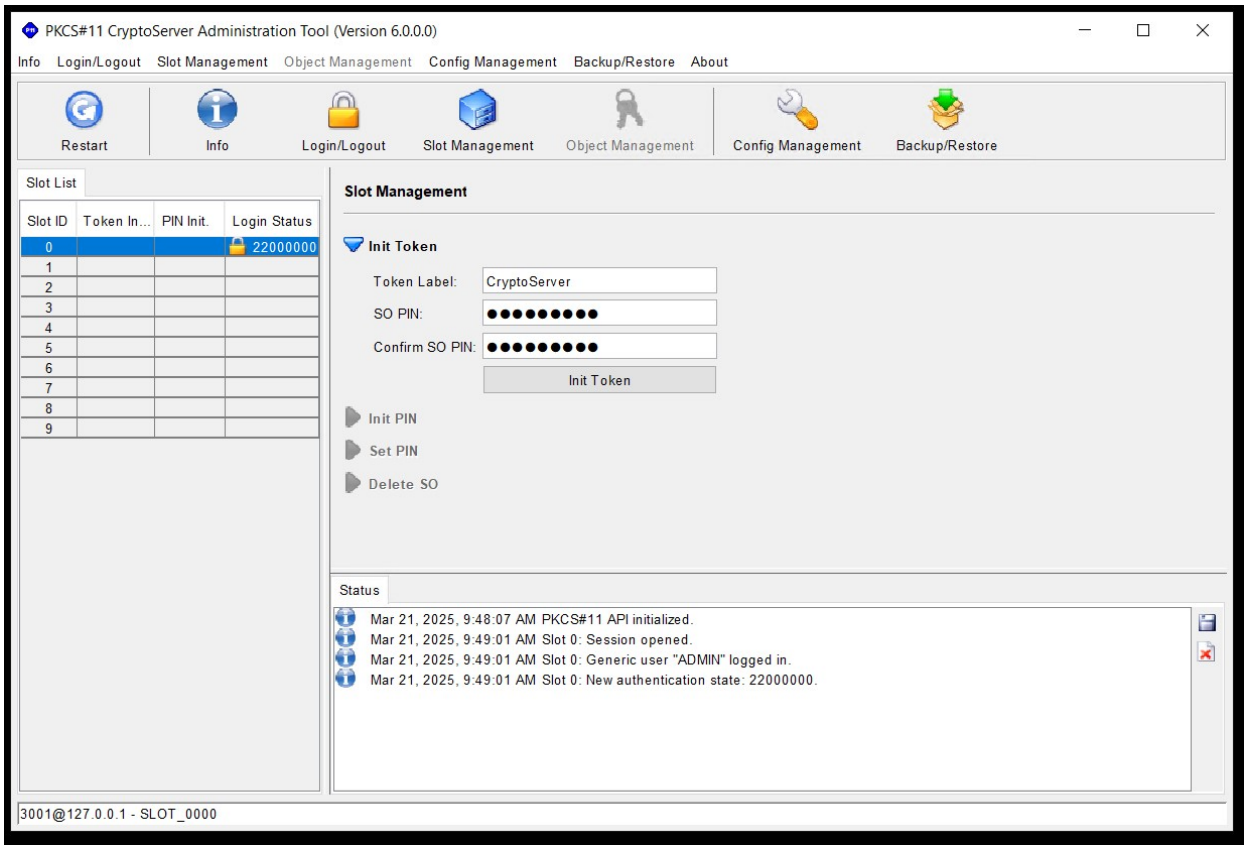
1. Open a command prompt as administrator and run the java -jar $_{p11cat.jar}$ command.
2. Log in as an administrator in CAT:

3. In the CAT, go to the **Slot List** tab and select Slot ID: 0. This is typically the default slot on the HSM.



4. Login to the Slot using the **ADMIN_SIM.key** file, which should have been copied to the *C:* drive. This key file is used to authenticate the administrator (SO) on the device.

5. Once logged in, navigate to the **Slot Management** tab to configure various settings for the Slot Token.



6. In the **Token Label** field, assign a label that will help identify the Slot Token(this will used in Secret Server).

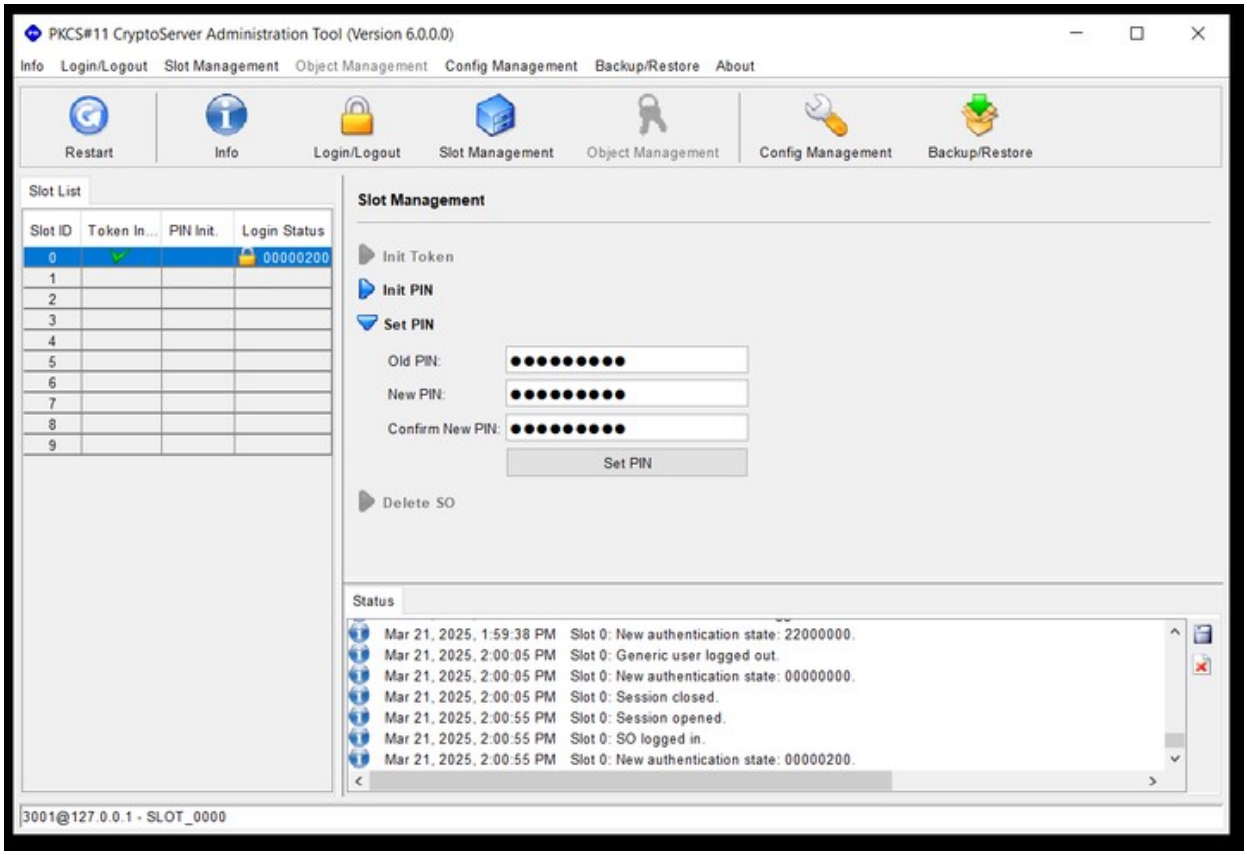
This label helps manage and identify the token easily in a larger security environment.

6. In the **SO PIN** field, enter the temporary PIN. The SO is responsible for initializing and managing the token, including creating the User (CO) PIN.

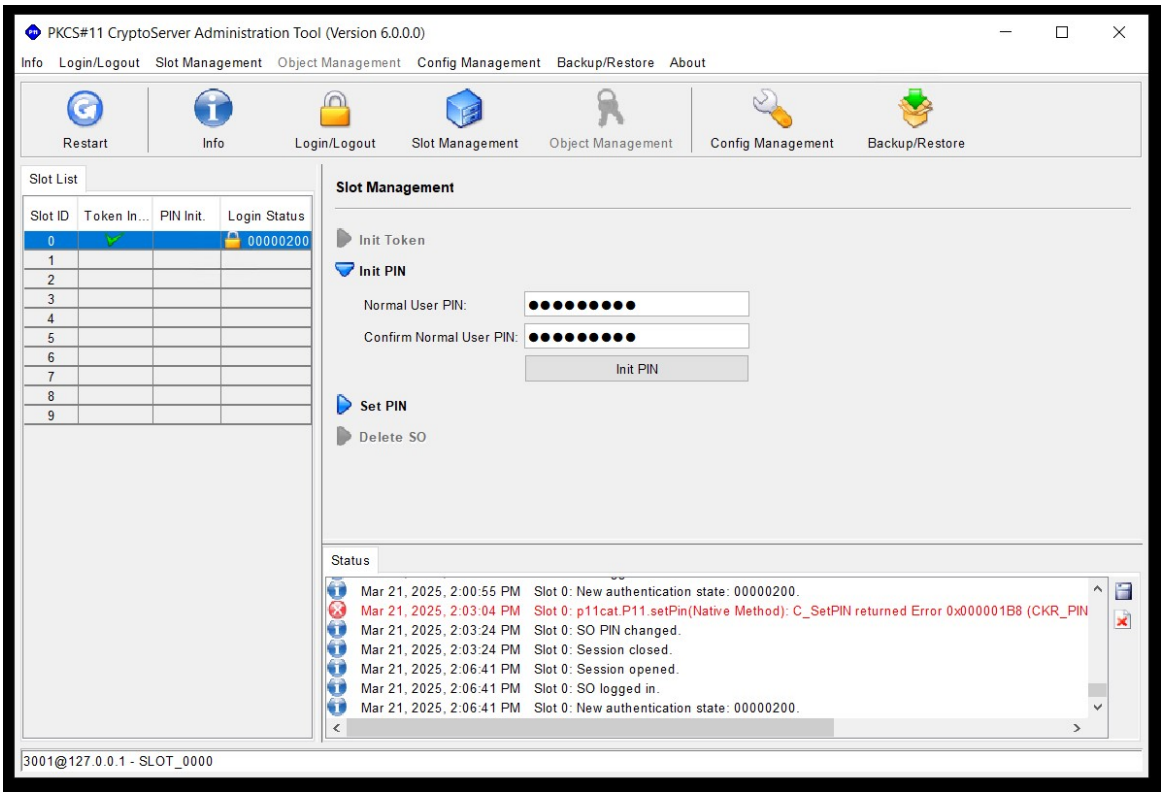
A typical SO PIN might be set to something secure, such as a 6- or 8-digit number, and it is essential to remember this PIN as it provides access to the token's administrative controls.

8. Select **Init Token**.
9. Go to the **Login/Logout** tab and then select **Logout All**.
10. Login as **SO User**.

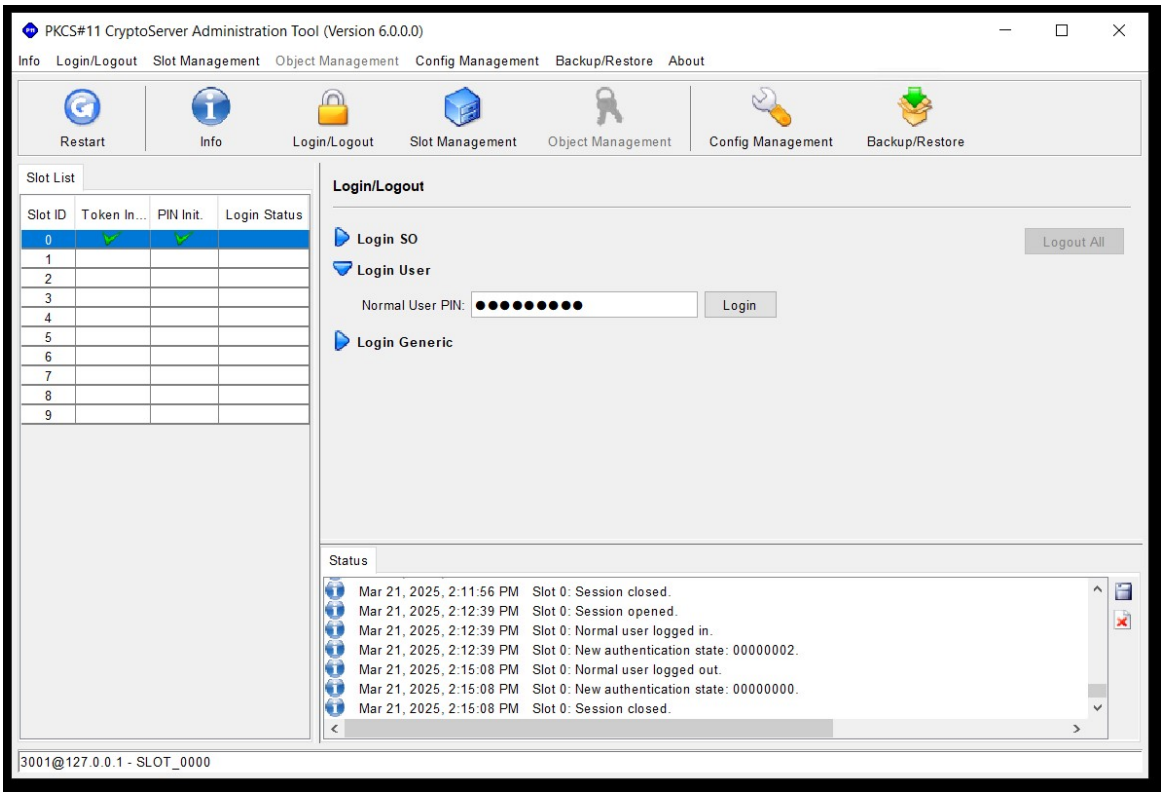
11. Set the **SO PIN**.



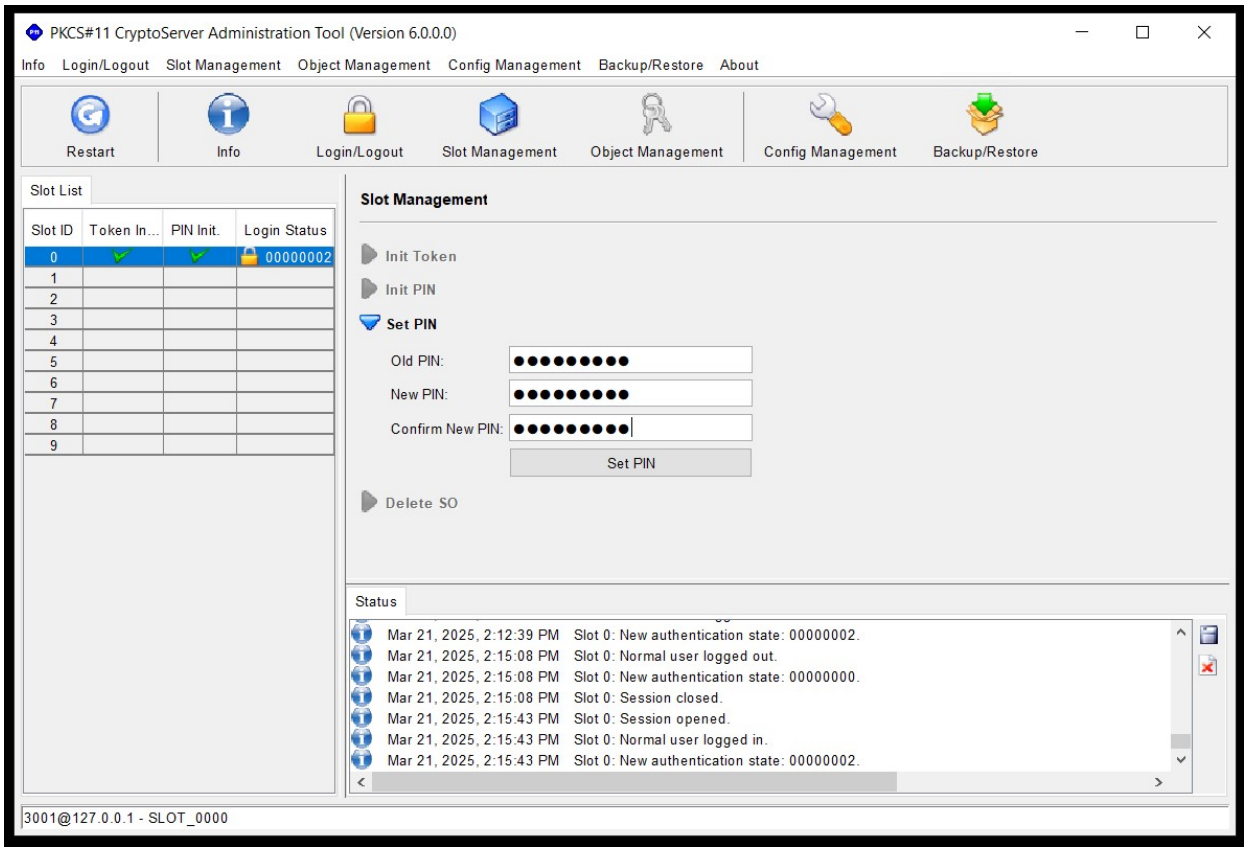
12. Go to the **Login/Logout** tab and then select **Logout All**.
13. Login as **SO User**.
14. Go to the **Slot Management** tab and expand the **Init PIN** section.
15. In the **Normal User PIN** field enter a temporary PIN and then confirm it.
16. Go to the **Login/Logout** tab and then select **Logout All**.
17. Login as **Crypto User**.
18. Go to the **Login/Logout** tab. The **Login/Logout** page opens.



19. Expand the **Login User** section.
20. In the **Normal User PIN** field type the previously created temporary PIN.
21. Select **Login**.
22. Go to the **Slot Management** tab.
23. Expand the **Set PIN** section, and enter the old PIN and then set a new PIN.
24. Select **Set PIN** to confirm the change of your PIN.



25. Go to the **Login/Logout** tab. The **Login/Logout** page opens.
26. Expand the **Login User** section.
27. In the **Normal User PIN** field enter the newly changed PIN.
28. Select **Login**.



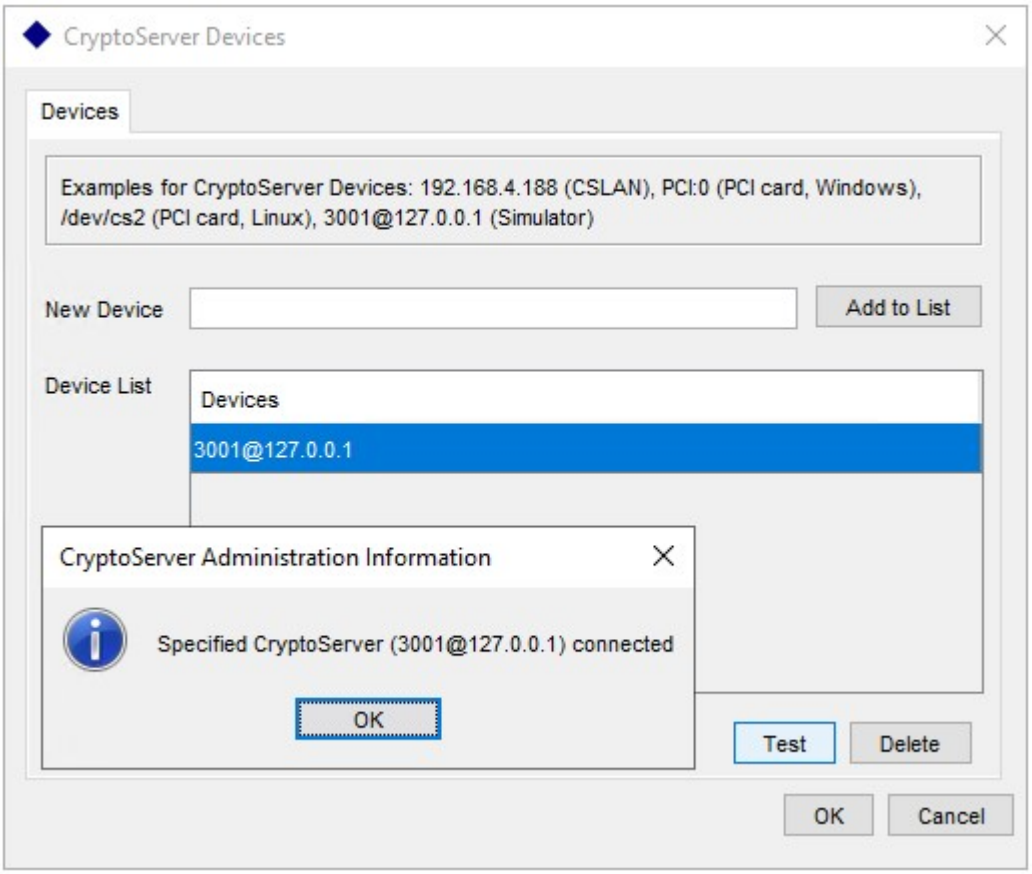
29. Select the **Object Management** tab. The **Object Management** page opens.
30. Select **Generate** to generate a key. This verifies if the Crypto User was setup properly.

CNG Setup

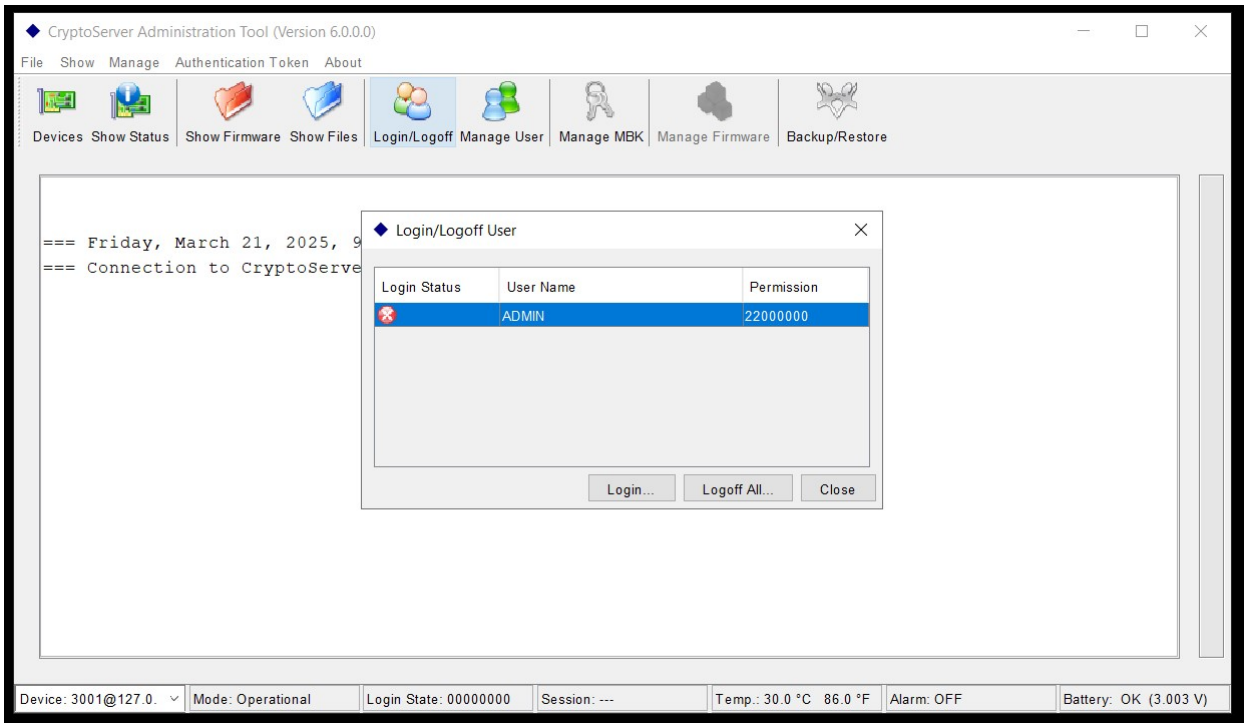
1. Open the CryptoServer Administration Tool (CAT) by selecting the CryptoServer Administration icon on your desktop.

or

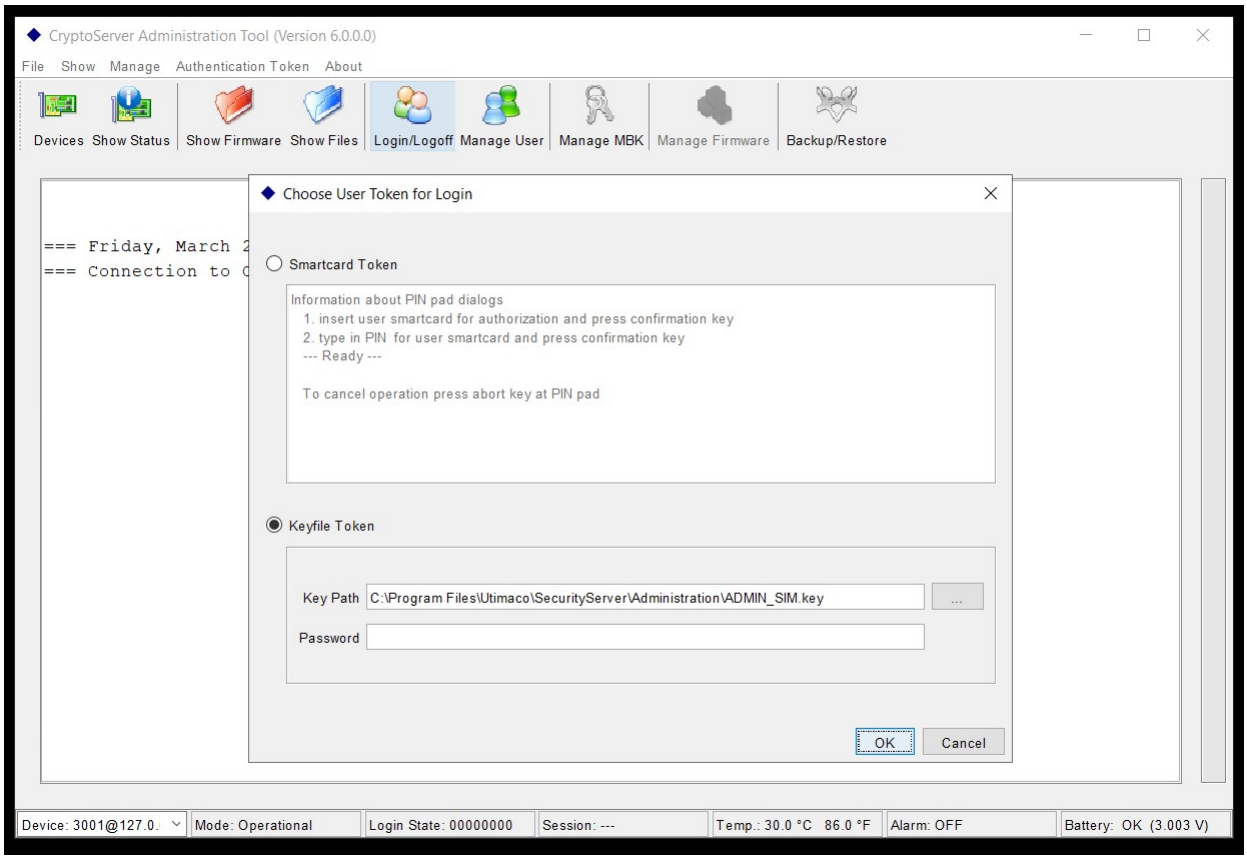
1. Open a command prompt as administrator and run the java -jar p11cat.jar command.
2. Select **Test** to ensure that you are connected to the HSM.



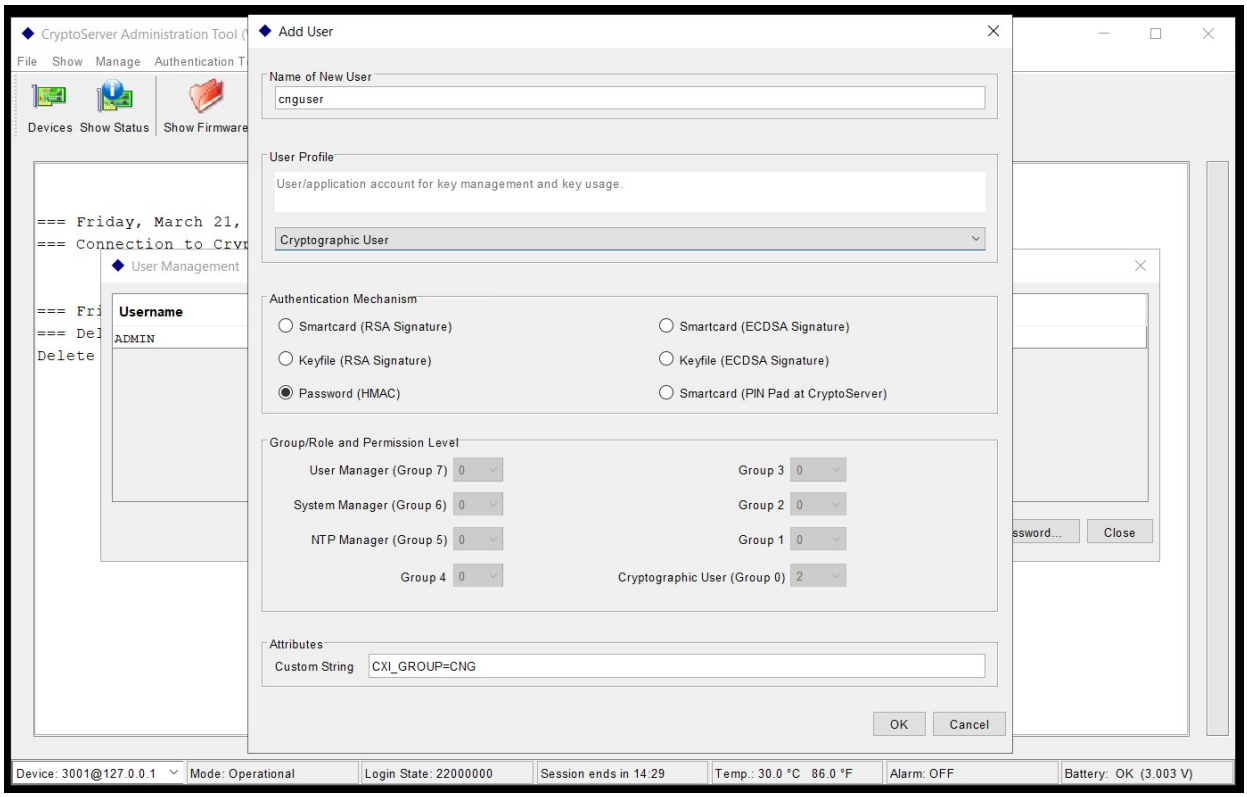
4. Select **Ok** to close the success token pop-up screen.
5. Select **Ok** in the **CryptoServer Devices** page to close the Devices modal.
6. Log in CryptoServer Administration Tool using the Admin user:
7. Select the **Login/Logout** tab.
8. In the users list, select **ADMIN**.



9. Select **Login**. The **Choose User Token for Login** page opens.
10. Select the **Keyfile Token** checkbox.
11. Select **Browse** and select the Keypath (browse to ADMIN_SIM.key in the C:\ drive), and leave the password blank.



12. Select **Ok**.
13. Select **Close** to the Login/Logoff User modal.
14. In the **Manage User** page, select **Add User** to start adding a CNG User. The **Add User** page opens.



15. In the **Name of New User** field, enter the name of the new user: **cnguser**.
16. Select the **Cryptographic User** in the **User Profile** dropdown list.
17. In the **Authentication Mechanism** section, select the **Password (HMAC)** checkbox.
18. In the **Attributes** section, in the **Custom String** field, enter the following: **CXI_GROUP=CNG**

Important: Make sure there are no spaces on either side or it will not work.

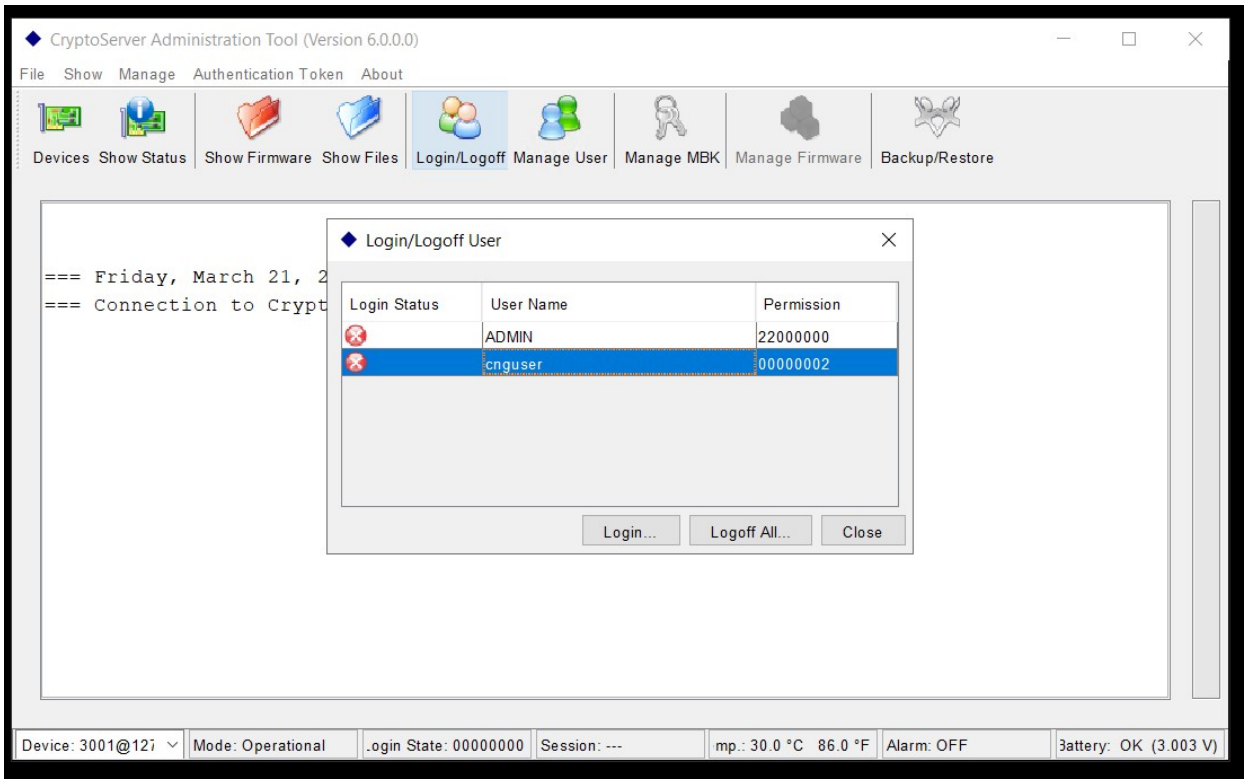
15. Select **Ok**.

Ensure user passwords are updated from the initial password before they can be used.

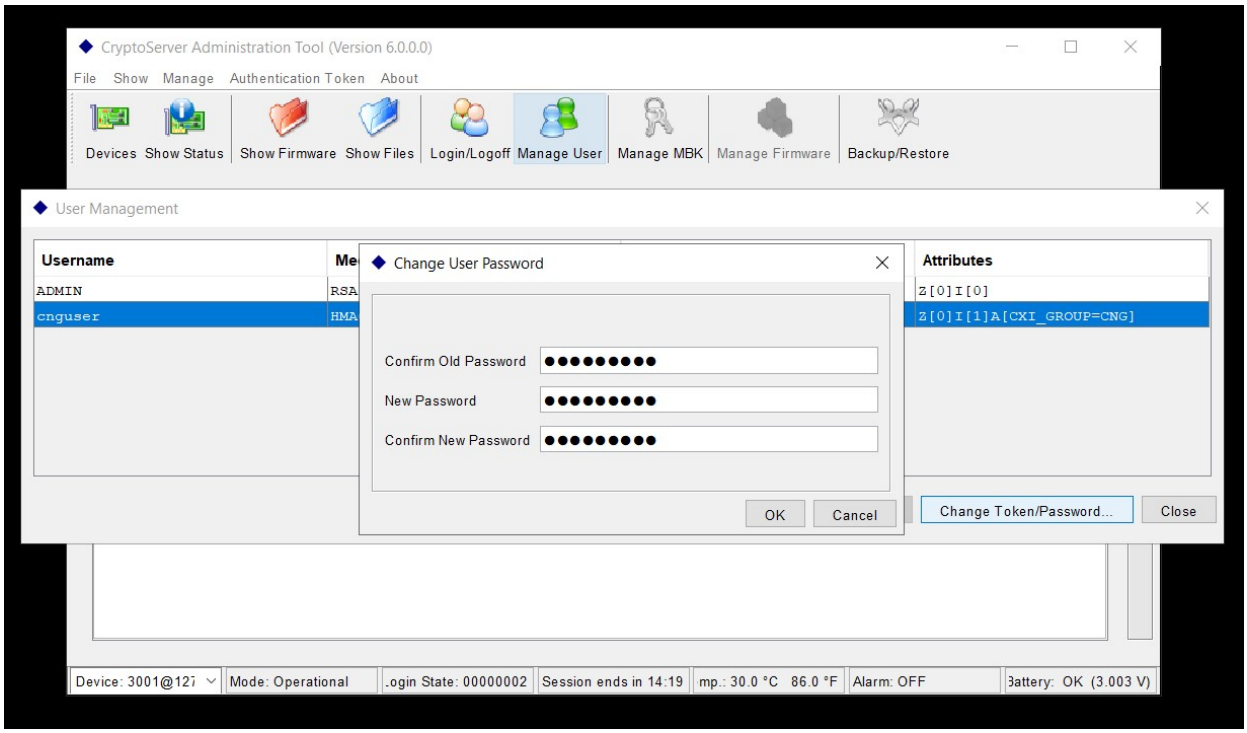
Update user credentials:

The user passwords must be updated from the initial password before they can be used. This ensures proper security and prevents errors like **"The user credentials need to be updated"** in CNG logs.

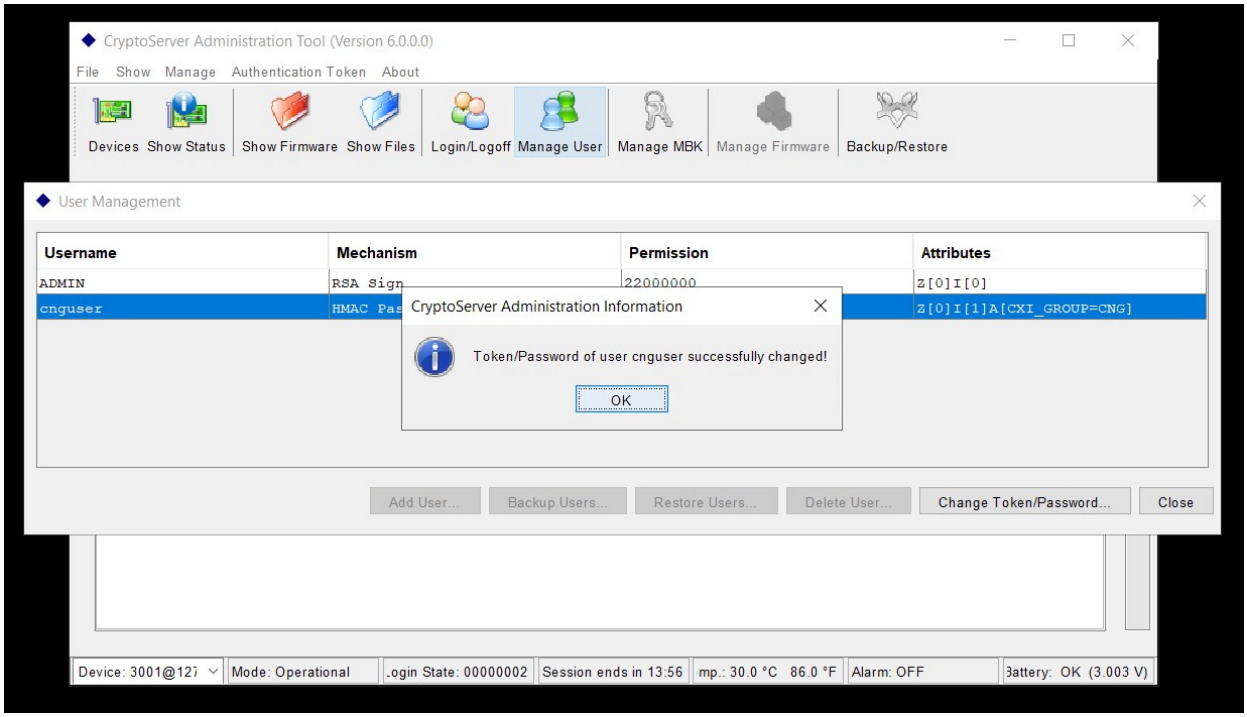
1. Launch CryptoServer Administration Tool (CAT) on your system.
2. Select **Login/Logoff** tab.
3. In the **Login/Logoff** page window, select **cnguser** from the list of available users.



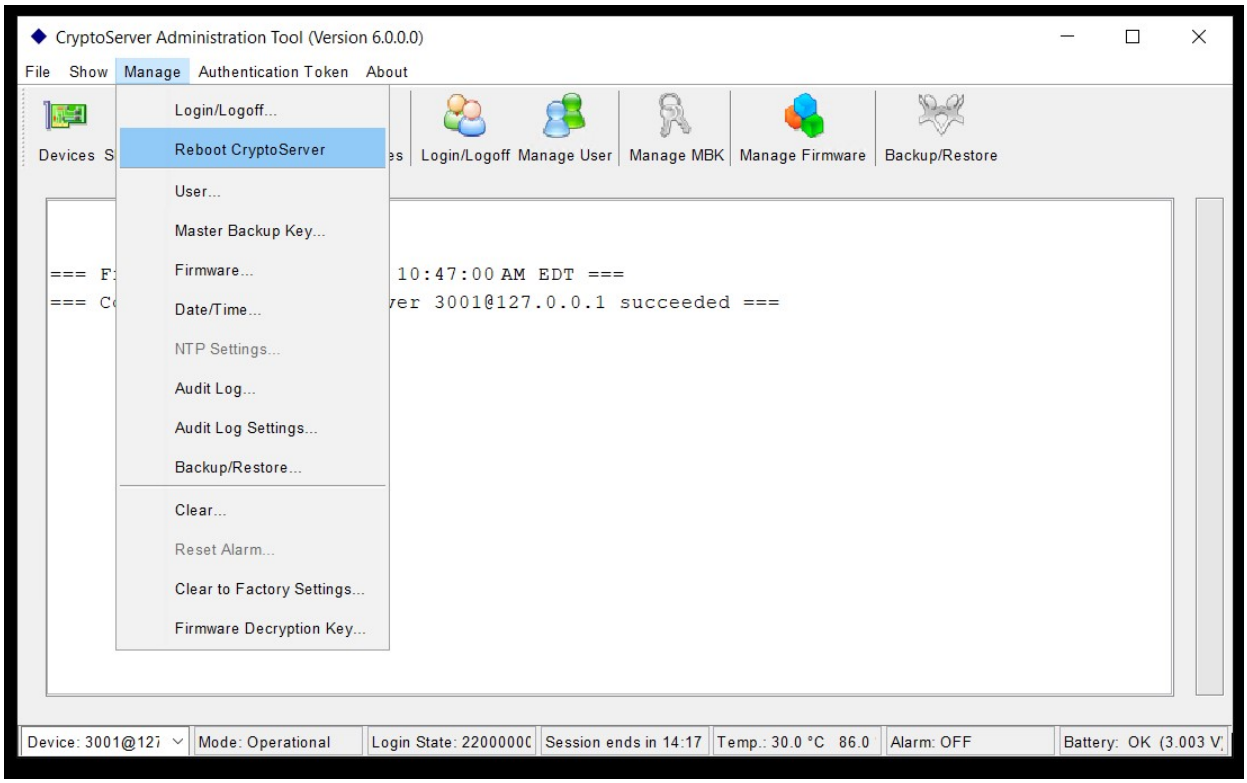
4. Select **Login...**.
5. After entering the password, select OK to log in.
6. Select **Close** to close the login window.
7. Select **Manage User** from the menu. The **User Management** page opens.
8. Select cnguser from the list of users.
9. Select **Token/Password**. The **Change User Password** page opens.
10. Enter the current password (initial password provided) and the new password for cnguser.



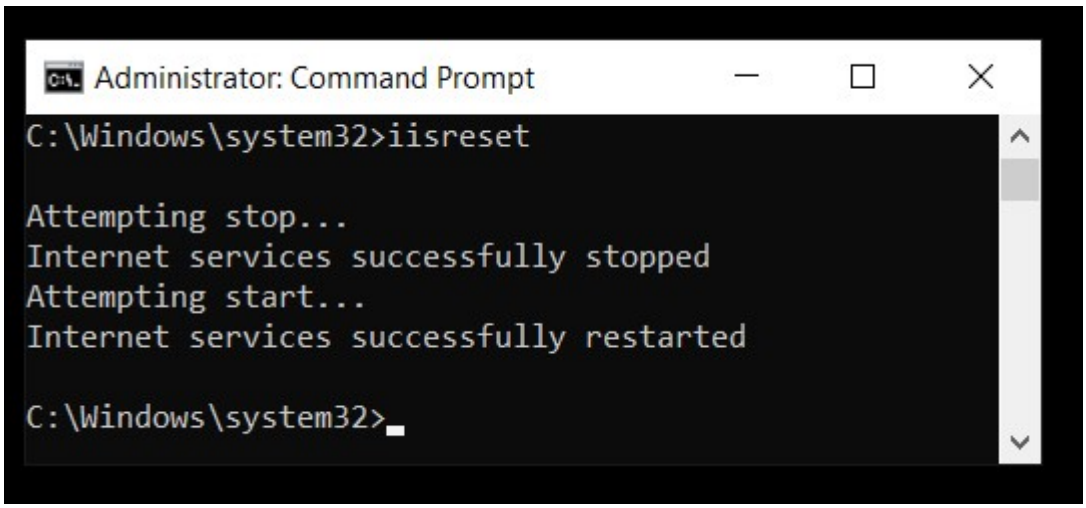
11. Select **Ok**. The following message will be displayed if the password was changed successfully:



12. Go to **Manage** and select **Reboot CryptoServer**.



13. Open the command line and perform an **iisreset** or recycle your application pool to finalize the setup.

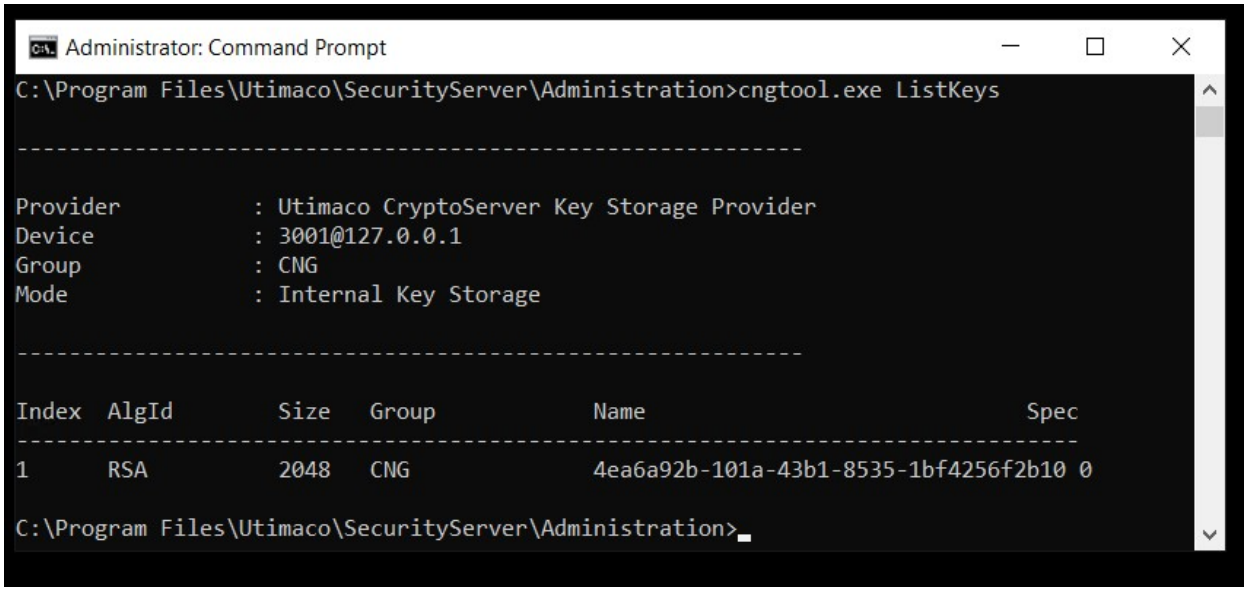


3.3 Managing Cryptographic Keys

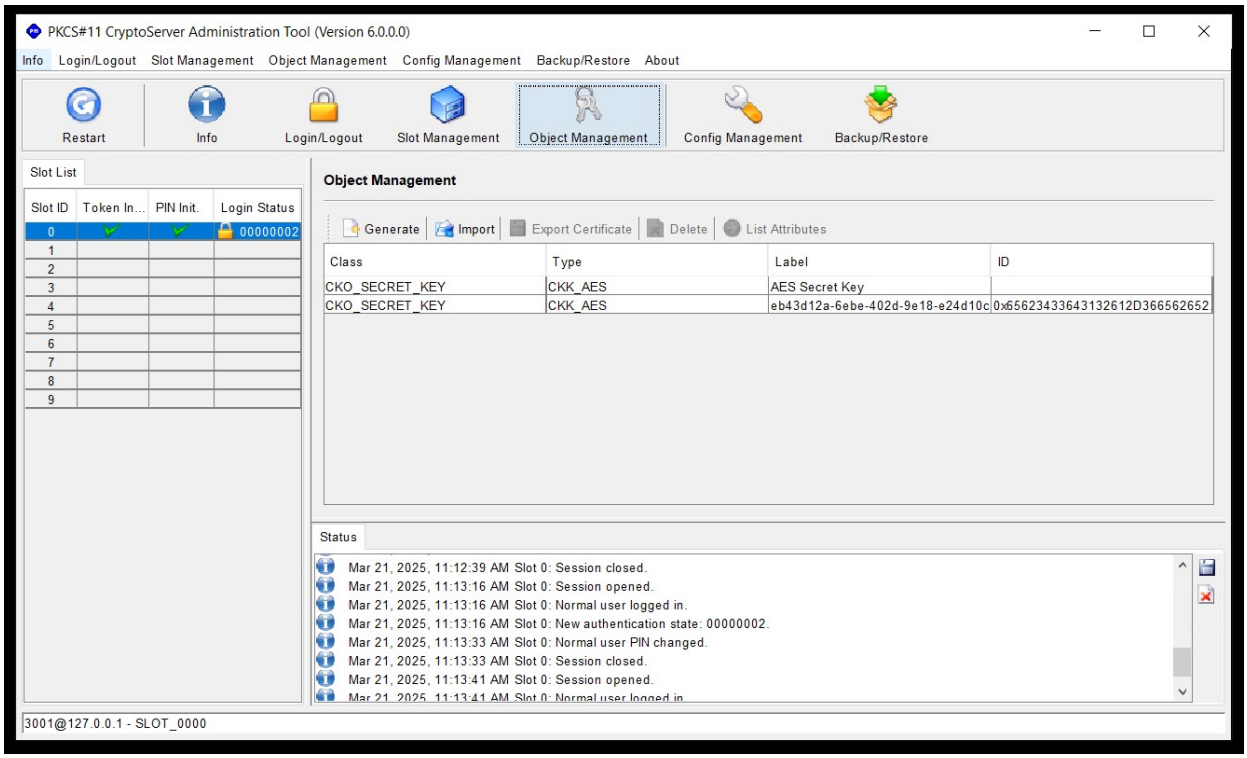
Once the users are created, configure the cryptographic algorithms, key types, and key storage.

1. For PKCS#11 and CNG, generate and manage keys as required using the CryptoServer Administration Tool and Secret Server.
2. To view or list generated keys:

- For CNG: l Use the cngtool.exe ListKeys command to view the created keys.



- For PKCS#11:
  - Use the PKCS11 CryptoServer Administration Tool (PKCS11 CAT) to view the keys.
  - Select the **Object Management** tab. The **Object Management** page opens. Here you can see the PKCS#11 keys.



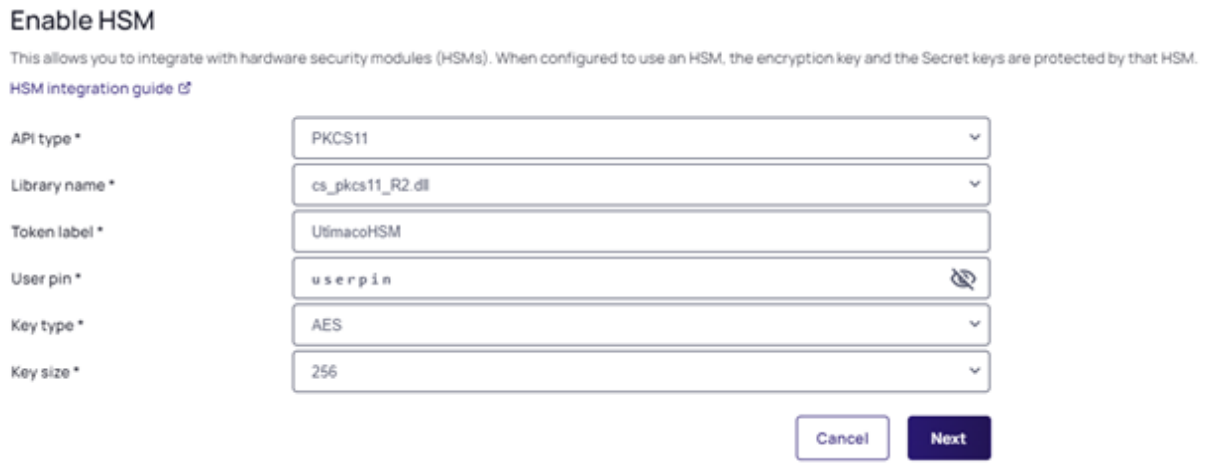
Only the Crypto Users can see these keys displayed in the Object Management page.

4 Configuring HSM in Secret Server

PKCS#11

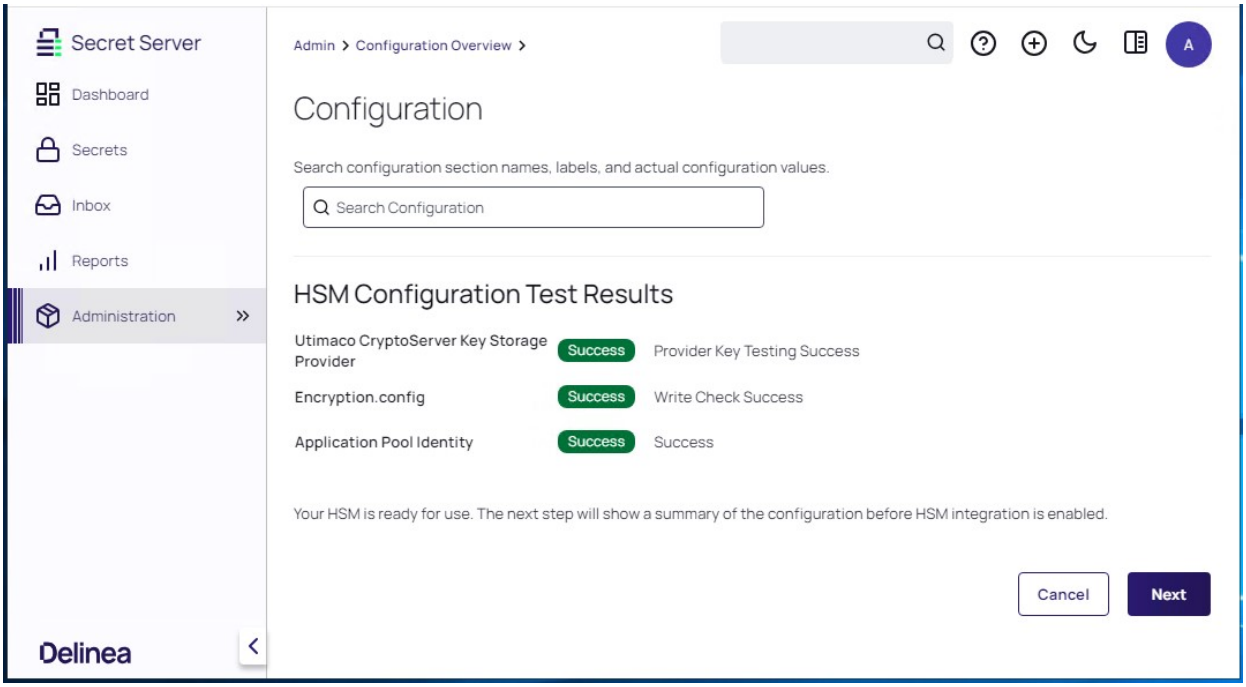
1. Open the Secret Server web application and log in with administrator access.
2. Navigate to **Settings -> Configuration -> General -> HSM**.
3. In HSM Configuration page, enable HSM if you haven't already.
4. Select API Type: PKCS#11 and provide the path to cs_pkcs11_R3.dll.
5. Enter Token Label and User Pin (from the PKCS#11 setup).

Example of PKCS#11 settings in Secret Server:



CNG

1. Open the Secret Server web application and log in with administrator access.
2. Navigate to **Settings -> Configuration -> General -> HSM**.
3. In HSM Configuration, enable HSM if you haven't already.
4. Select the **Utimaco CryptoServer Key Storage Provider** option, a CNG-based service provider.
5. Choose a key size of 2048 or 4096.
6. Select **Next**.
7. If the Secret Server is successfully connected to HSM the following message is displayed:



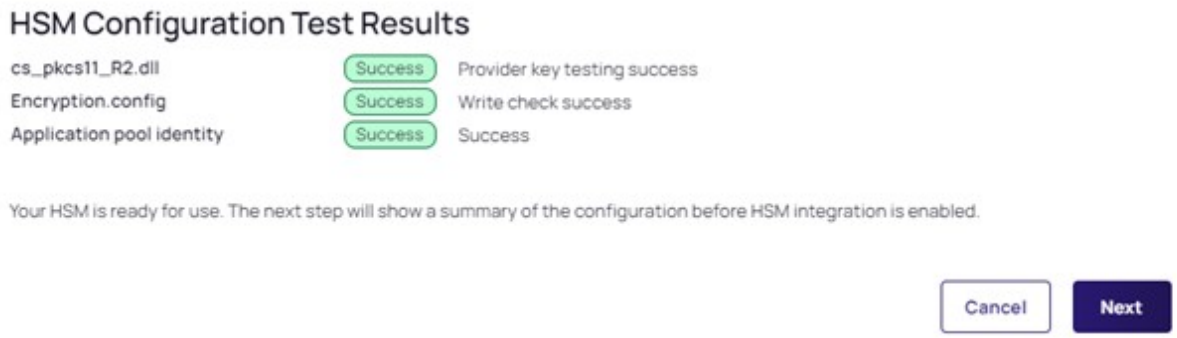
For more information about HSM configuration in Secret Server, click here.

5 Verification in Secret Server

To verify the integration:

1. Go to the **HSM configuration** page in Secret Server.

2. Select the **Enable HSM** option, and follow the steps.



6 Troublehshooting

If you encounter issues with user credentials or integration, ensure that:

- The **Token/Password** has been updated.
- The correct **Keyfile Token** has been selected during log in.