

Prerequisites:

To get the PKCS#11 Engine working smoothly with your Utimaco HSM and Encryption Consulting's CodeSign Secure, you'll need a few key things. Here are the steps to install the resources that are essential for setting up the **Windows** environment:

1. Utimaco Security Server

Utimaco SecurityServer provides cryptographic libraries, tools, and interfaces (e.g., PKCS#11, CSP, and JCE) to manage keys and perform cryptographic operations securely. The software includes the CryptoServer SDK, administrative tools, and simulators, facilitating seamless HSM integration for enhanced security and regulatory compliance.

Installation Steps:

Step 1: Download the Provider

- Download the provider (e.g., SecurityServerEvaluation-V6.1.1 for Windows) from the Utimaco customer portal.

Step 2: Install the Provider

- Extract the downloaded package, run the MSI installer, and follow the prompts to set up the Utimaco Security Server on your system.
- It will install the required tools to the default location (C:\Program Files\Utimaco), unless otherwise specified while installing, and will also create shortcuts for the following tools on the current user's Desktop for easier access:
 - CryptoServer Administration
 - PKCS#11 CryptoServer Administration
 - CryptoServer Simulator
- Along with this, it will also modify the Environment Variables with the Utimaco SecurityServer's selected locations and configuration files.

2. OpenSSL 3.x:

OpenSSL 3.x is required for cryptographic operations and to leverage the PKCS#11 provider with the Utimaco HSM.

Installation Steps:

Step 1: Download OpenSSL

- Download the latest 64-bit OpenSSL 3.x installer for Windows using this [link](#).

Step 2: Install OpenSSL

- Run the downloaded installer with administrative privileges.
- Choose the default installation directory (C:\Program Files\OpenSSL-Win64) unless you have specific requirements.

Step 3: Configure Environment Variable

- Add the OpenSSL binary directory to the system PATH:
 - C:\Program Files\OpenSSL-Win64\bin

Step 4: Verification

- Open a new Command Prompt and run the following command to test openssl installation.
 - openssl version

3. Java Runtime Environment

Utimaco SecurityServer also requires a Java Runtime Environment (Tested version Java 15). Refer to the below matrix to check the Java compatible version:

Java Runtime Environment	Version
Oracle Java	8,11,15
OpenJDK	8,11,15

Installation Steps:

Step 1: Download Java 15

- Download the compatible Java executable from [here](#) for your Windows system.

Step 2: Install Java 15

- Run the downloaded executable and follow the prompts to set up Java 15.

Step 3: Verification

- Open a new Command Prompt and run the following command to test java installation.
 - java -version

4. Microsoft Visual Studio Build Tools

Microsoft Visual Studio Build Tools are required to compile the OpenSC PKCS#11 Wrapper Library (libp11) on Windows

Installation Steps:

Step 1: Download Visual Studio Build Tools

- Download the Microsoft Build Tools for Visual Studio 2022 using this [link](#).

Step 2: Install Build Tools

- Run the installer (vs_buildtools.exe) with administrative privileges.

Step 3: Verify Installation

- Open the “**x64 Native Tools Command Prompt**” from the Start menu and run
 - `nmake /?`

This should display the help for the nmake utility, confirming the build tools are installed.

NOTE: “x64 Native Tools Command Prompt” should be present inside C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Visual Studio 2022\Visual Studio Tools\VC

5. OpenSC PKCS#11 Wrapper Library

The OpenSC PKCS#11 Wrapper Library (libp11) provides the PKCS#11 engine plugin (pkcs11.dll) for OpenSSL to interact with the HSM.

Installation Steps:

Step 1: Download the Source Code

- Clone the OpenSC/libp11 repository from GitHub or download it as a ZIP file.
- Clone using Git (if installed):
 - `git clone https://github.com/OpenSC/libp11.git`
C:\Users\<Username>\source\repos\libp11
- Or download the ZIP from this [link](#) and extract it to C:\Users\<Username>\source\repos\libp11.

Step 2: Compile the Library

- Open the “x64 Native Tools Command Prompt”.
- Navigate to the libp11 directory
 - `cd “C:\Users\<Username>\source\repos\libp11”`

- Run the nmake command to build the library
 - nmake /f Makefile.mak OPENSSL_DIR="C:\Program Files\OpenSSL-Win64" BUILD_FOR=WIN64
- **NOTE:** Ensure OPENSSL_DIR points to your OpenSSL installation directory.

Step 3: Verify Compilation

- Check for the pkcs11.dll file in the libp11\src folder. This is the OpenSC PKCS#11 Engine Plugin.

Step 4: Copy the SRC folder

- Copy the src folder that you just created to your OpenSSL bin directory, i.e., C:\Program Files\OpenSSL-Win64\bin

Configuration

After installing the prerequisites, you need to configure the Utimaco SecurityServer, OpenSSL, and the OpenSC PKCS#11 Wrapper Library to enable communication with your Utimaco HSM.

1. Configure the Utimaco SecurityServer

Configuring Utimaco SecurityServer requires setting up environment variables, updating configuration files (e.g., PKCS#11 settings), to manage HSM access and operations securely.

Steps:

Step 1: Locate the Configuration File (cs_pkcs11_R3.cfg)

- Navigate to the Utimaco PKCS#11 Provider installation directory, typically:
 - C:\ProgramData\Utimaco\PKCS11_R3

Step 2: Update the IP address of the HSM

- Under the [HSMCluster] section, update the IP address of your Utimaco HSM. Remember to uncomment (remove the hash symbol) the line (e.g., Devices=3001@127.0.0.1) where you have added the IP.

```

cs_pkcs11_R3.cfg
C:\ProgramData\Utimaco>PKCS11_R3> cs_pkcs11_R3.cfg
66 [HSMCluster]
67 # Device specifier (here: internal PCI device)
68 # For Unix:
69 #Devices = /dev/cv2.0
70
71 # For Windows:
72 #Devices = PCI:0
73
74 # Device specifier (here: cHSM on local u.trust Anchor device - last number represents cHSM slot (1))
75 #Devices = /dev/cv2.0.1
76
77 # Device specifier (here: local simulator)
78 #Devices = 3001@127.0.0.1
79
80 # Device specifier (here: cluster of simulators)
81 #Devices = { 3001@127.0.0.1 3003@127.0.0.1 }
82
83 # Device specifier (here: cHSM on remote u.trust Anchor device - port = base port (4000) + cHSM slot (1))
84 #Devices = 4001@192.168.0.1
85
86 # Device specifier (here: remote device with IP address 192.168.0.1)
87 #Devices = 192.168.0.1
88
89 # Device specifier (here: cluster of remote devices - first as above, others using format <port>@<ip>)
90 #Devices = { 192.168.0.1 288@192.168.0.2 4001@192.168.0.3 }

```

Here, we will be using a local simulator that runs, by default, on localhost (127.0.0.1) port 3001.

2. Create User Roles for a Slot

To generate keys and certificates using Utimaco SecurityServer, you will need to create and define user roles—Admin, Security Officer (SO), and Cryptographic User

Steps:

Step 1: Start the CryptoServer Simulator

- Start the CryptoServer Simulator, provided on the Desktop, to initialize the required settings.

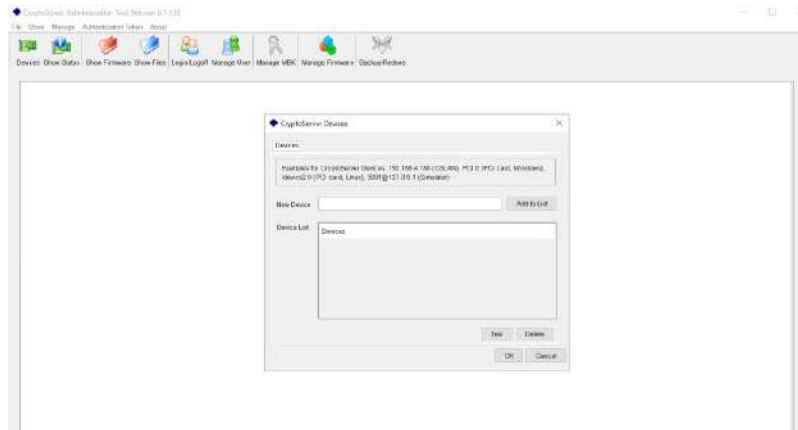
```

Utimaco CryptoServer SDKS - Simulator 3001@localhost
C:\Program Files\Utimaco\SecurityServer\Simulator\bin>.bl_sim.exe -h -o -d "C:\ProgramData\Utimaco\Simulator\devices"
Utimaco CryptoServer Simulator HSO process started

25.05.29 23:53:13 SNOS SDK Ver. 5.7.1.1 (Mar 18 2025) started [0]
25.05.29 23:53:13 Compiler Ver. 19.0
25.05.29 23:53:13 CPU clock frequency: 10000000
25.05.29 23:53:13 Devices directory: 'C:\ProgramData\Utimaco\Simulator\devices'
25.05.29 23:53:14 Sensory Controller Ver. 2.0.0.42 [0/0]
25.05.29 23:53:14 Real Random Number Generator initialized with:
  RESEED_INTERVAL = 1000
  PREDICTION_RESISTANCE = 0
  REALRANDOM_SHARE = 3
25.05.29 23:53:14 Pseudo Random Number Generator initialized with:
  RESEED_INTERVAL = 1000
  PREDICTION_RESISTANCE = 0
  REALRANDOM_SHARE = 0
25.05.29 23:53:14 Load module 'adr.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'cnd.msc' from FLASHFILE
25.05.29 23:53:14 CHDS: .pscf support enabled
25.05.29 23:53:14 Load module 'crypt.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'cxi.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'db.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'mbx.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'pcca.msc' from FLASHFILE
25.05.29 23:53:14 Load module 'pp.msc' from FLASHFILE

```

NOTE: In case you using an actual Utimaco HSM, you will need to start the CryptoServer Administrator application, also present on the Desktop.



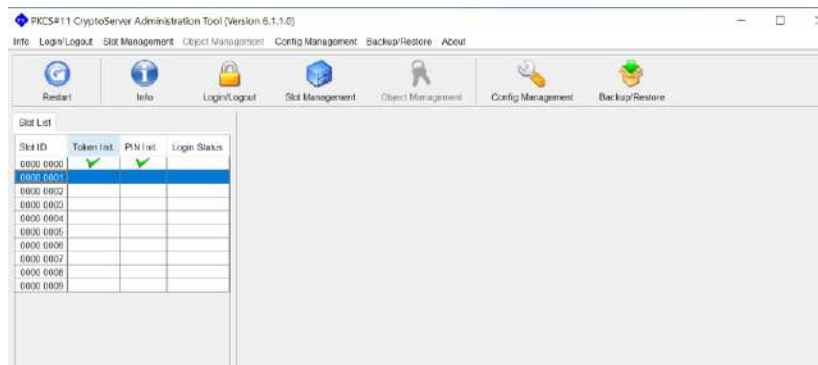
Step 2: Locate the PKCS#11 CryptoServer Administration Application

- Open the PKCS#11 CryptoServer application, typically provided on the user's Desktop



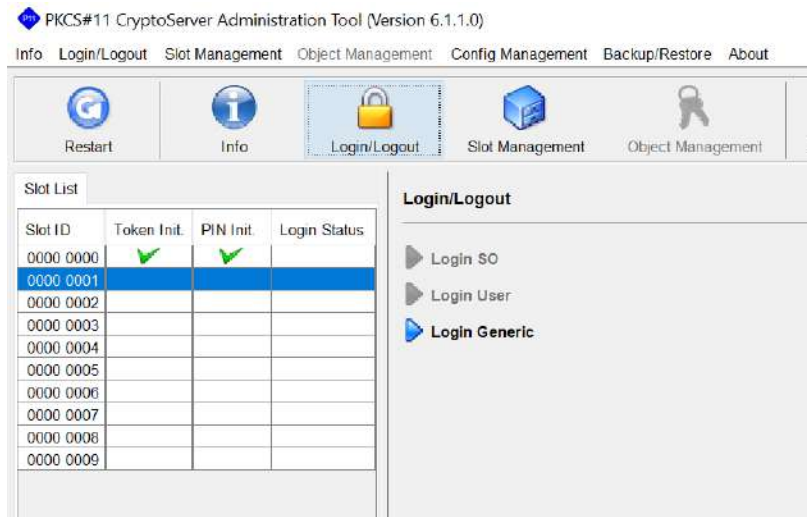
Step 3: Select the Required Slot

- From the left side table, click on the required slot number. Here, we have selected slot number 1

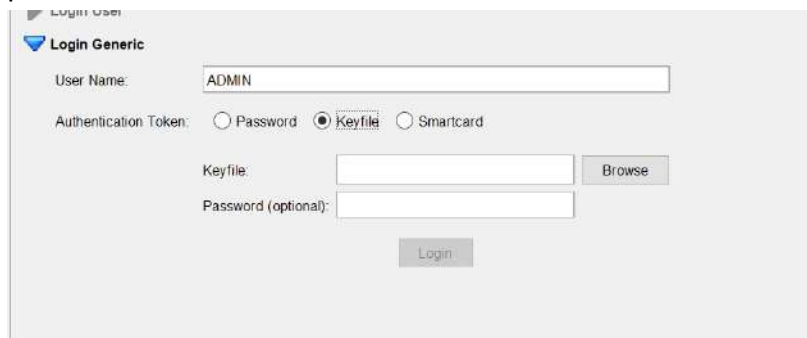


Step 4: Log in as the ADMIN

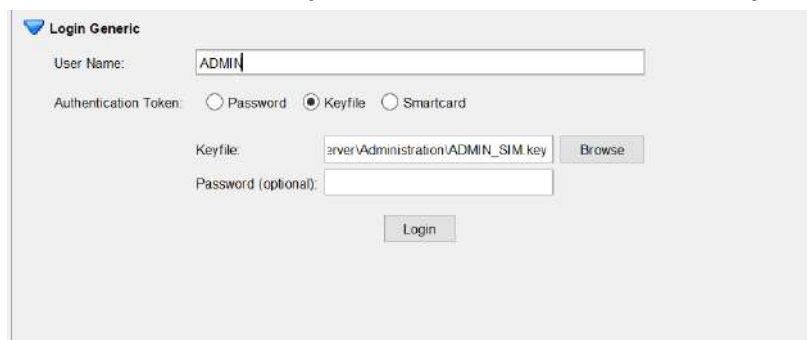
- Go to the Login/Logout section from the top bar and select the "Login Generic" option.



- Enter “ADMIN” as the username and select “Keyfile” option for the password.



- Browse the Keyfile and provide the password file. When running the simulator, select the “ADMIN_SIM.key” file; otherwise, use the “ADMIN_EC.key”. These key files are usually present in the “C:\Program Files\Utlimaco\SecurityServer\Administration” directory.



- Click Login to log in as the ADMIN user. It will show you a lock in the Login Status in the left table for that slot.

Slot List				Login/Logout	
Slot ID	Token Init.	PIN Init.	Login Status		
0000 0000	✓	✓		Login SO	
0000 0001			22000000	Login User	
0000 0002				Login Generic	
0000 0003					
0000 0004					
0000 0005					
0000 0006					
0000 0007					
0000 0008					
0000 0009					

Step 5: Initialize the Token for this slot

- Open the Slot Management section from the top bar and select the “Init Token” option.

The screenshot shows the 'Slot Management' section of the application. The 'Init Token' option is selected, and the 'Token Label' field is populated with 'CryptoServer PKCS11 Token'. The 'SO PIN' and 'Confirm SO PIN' fields are empty. The 'Init Token' button is visible at the bottom of the form.

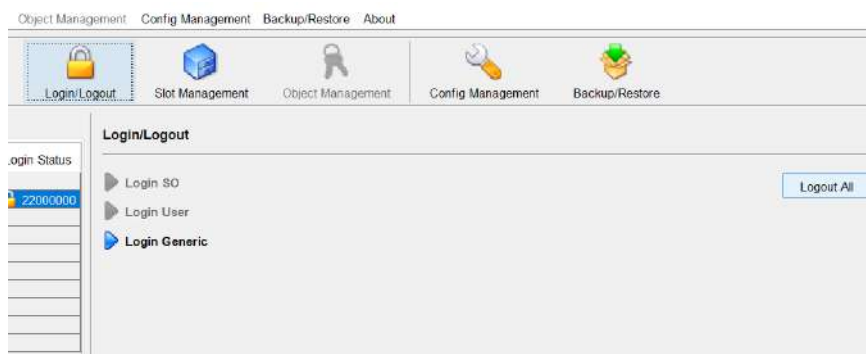
- Enter the required token name for this slot and provide a temporary PIN for the Security Officer role (this PIN will be changed in the later steps)

The screenshot shows the 'Slot Management' section of the application. The 'Init Token' option is selected, and the 'Token Label' field is populated with 'UtimacoTest'. The 'SO PIN' and 'Confirm SO PIN' fields are filled with a temporary PIN (represented by black dots). The 'Init Token' button is visible at the bottom of the form.

- Click on the “Init Token” button to finalize the token. It will now disable the “Init Token” option for this slot and enable the “Delete SO” option.



- Now, go to the Login/Logout section and click on the “Logout All” option to log out all the active user roles.

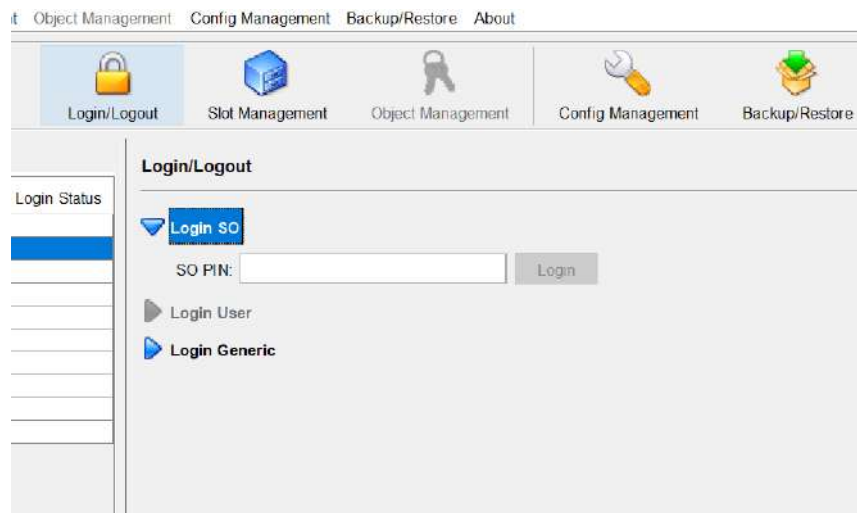


- It will show a green check mark in the left table under Token Init for this slot.

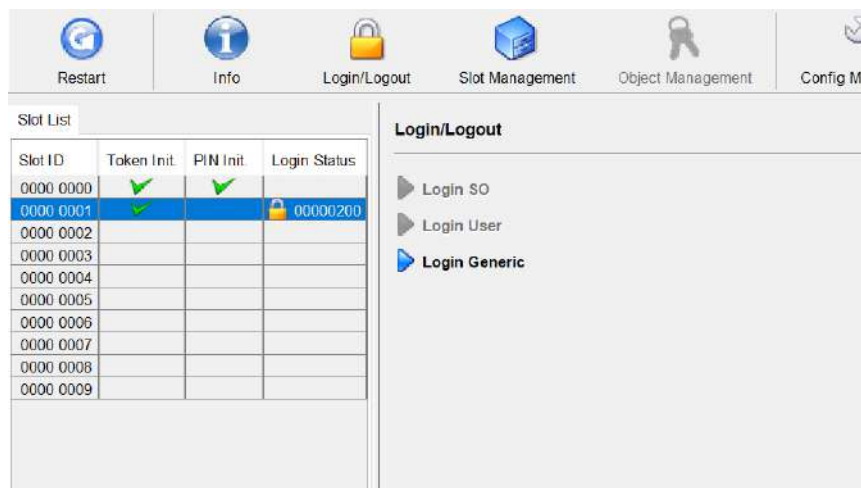
Slot List			
Slot ID	Token Init.	PIN Init.	Login Status
0000 0000	✓	✓	
0000 0001	✓		
0000 0002			
0000 0003			
0000 0004			
0000 0005			
0000 0006			
0000 0007			
0000 0008			
0000 0009			

Step 6: Set up the Security Officer role

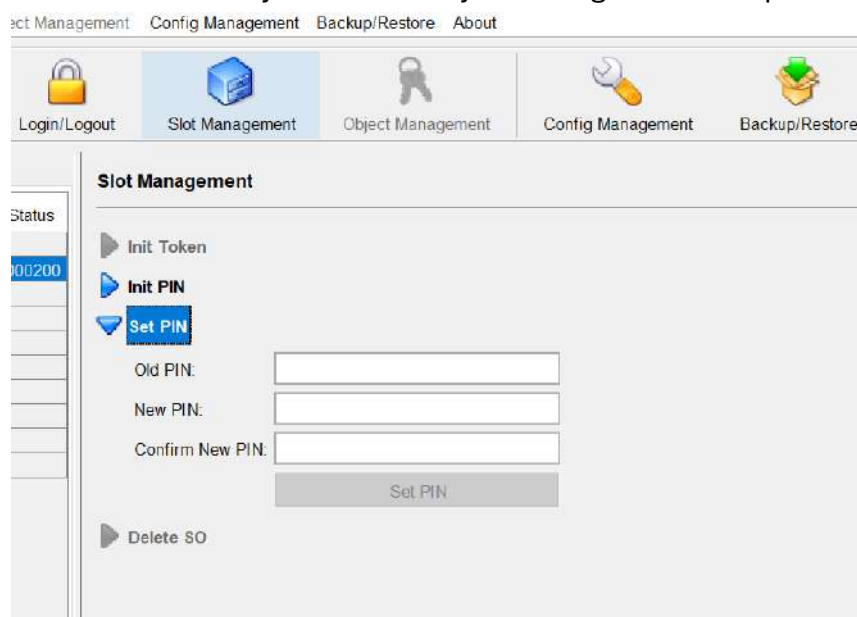
- Go to the “Login/Logout” section and select the “Login SO” option.



- Enter the temporary SO PIN that you had set up in the earlier step for the Security Officer role and click “Login” button. It will show you a lock symbol in the left table under “Login Status”.



- Now, go to the Slot Management section from the top bar, and set a new PIN for the Security Officer role by selecting “Set PIN” option.



- Set a new SO PIN for this slot's Security Officer.

Slot Management

Init Token

Init PIN

Set PIN

Old PIN: [Masked PIN]

New PIN: [Masked PIN]

Confirm New PIN: [Masked PIN]

Set PIN

Delete SO

- It will log you out from the current session as the SO, which you can see from the “Login/Logout” section or the left side table’s “Login Status” column.

Login/Logout

Restart Info Login/Logout Slot Management Object Management Config Management Backup/Restore

Slot ID	Token Init	PIN Init	Login Status
0000 0000	✓	✓	
0000 0001	✓		
0000 0002			
0000 0003			
0000 0004			
0000 0005			
0000 0006			
0000 0007			
0000 0008			
0000 0009			

Login SO
 Login User
 Login Generic

- Log in again as the SO with the new SO PIN by selecting “Login SO” in the “Login/Logout” section.

Login/Logout

Login SO

SO PIN: [Masked PIN] Login

Login User

Login Generic

- It will show you a lock in the left side table on successful log in.

Slot List				Login/Logout	
Slot ID	Token Init.	PIN Init.	Login Status		
0000 0000	✓	✓		Login SO	
0000 0001	✓	✓	00000200	Login User	
0000 0002				Login Generic	
0000 0003					
0000 0004					
0000 0005					
0000 0006					
0000 0007					
0000 0008					
0000 0009					

Step 7: Set up the Cryptographic User role

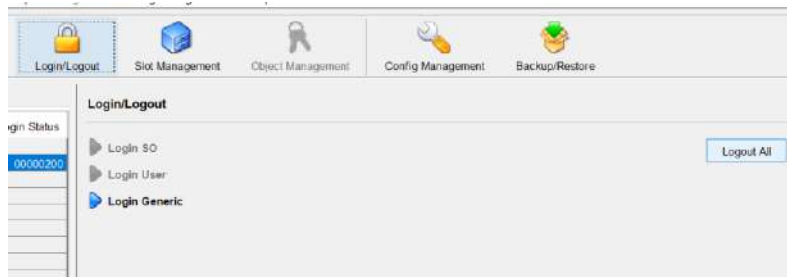
- Go to the “Slot Management” section and select the “Init PIN” option.

The screenshot shows the 'Slot Management' section of the interface. The 'Init PIN' option is selected, and the 'Normal User PIN' and 'Confirm Normal User PIN' fields are visible. The 'Init PIN' button is highlighted.

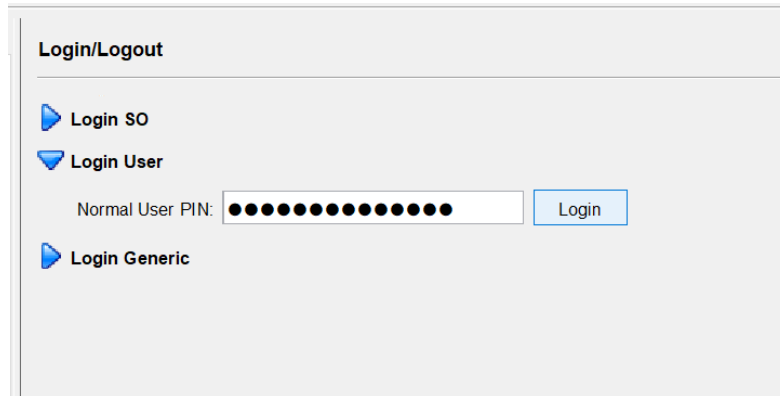
- Enter a temporary PIN for the cryptographic user for this slot and click on “Init PIN” button.

The screenshot shows the 'Slot Management' section of the interface. The 'Init PIN' option is selected, and the 'Normal User PIN' and 'Confirm Normal User PIN' fields are visible. The 'Init PIN' button is highlighted.

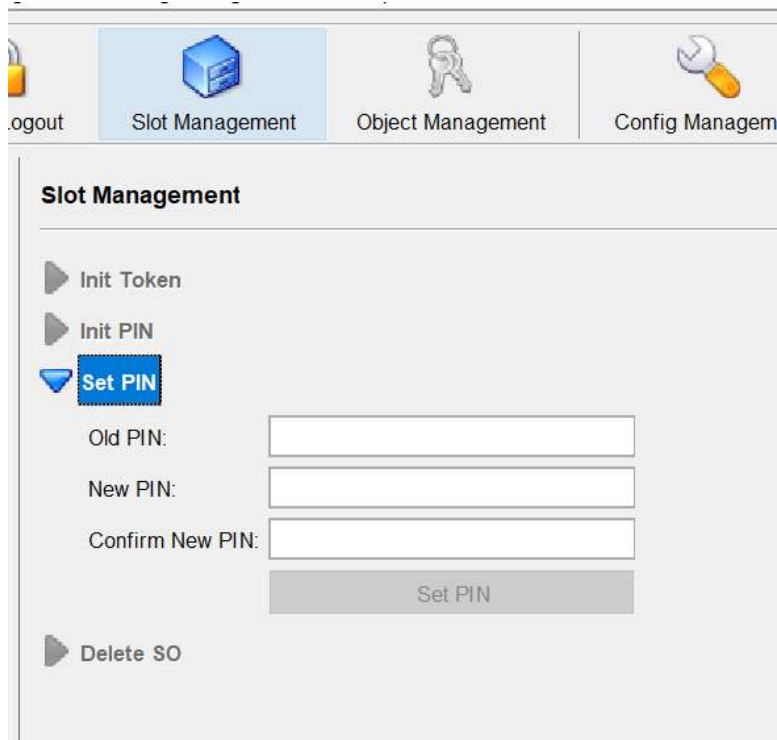
- Now log out all active sessions from the “Login/Logout” section.



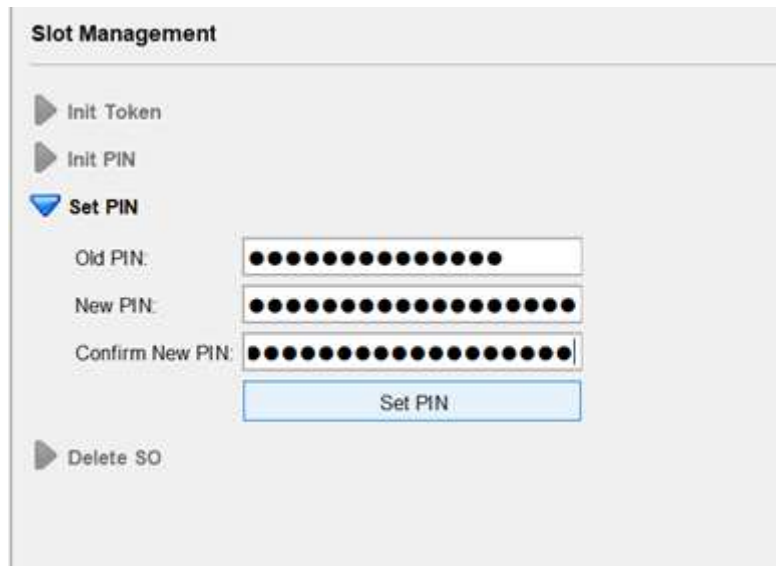
- Now log in as the Cryptographic User using the temporary PIN by selecting the “Login User” option in the “Login/Logout” section.



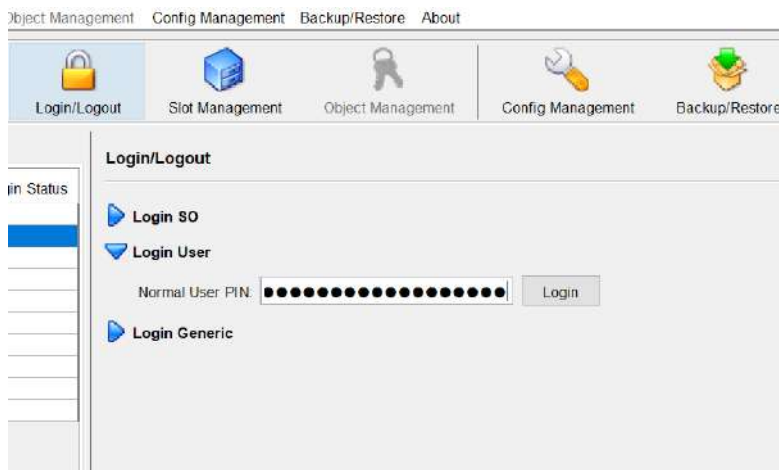
- Go to the “Slot Management” section and set up a new PIN for the cryptographic user using the “Set PIN” option.



- Update the PIN for the cryptographic user in this slot



- This will log you out of your current session. Log in again as the user from the “Login/Logout” section.



- You are ready with all the required roles for this slot. You will need to be logged in as the Cryptographic User to perform any object management, such as key or certificate generation.

3. Configure OpenSSL to Use the PKCS#11 Engine

OpenSSL must be configured to load the Utimaco PKCS#11 Provider (cs_pkcs11_R3.dll) and the OpenSC PKCS#11 Engine Plugin (pkcs11.dll) to perform cryptographic operations with the HSM.

Steps:

Step 1: Locate the OpenSSL Configuration File (openssl.cfg)

- Find the OpenSSL configuration file:
 - C:\Program Files\Common Files\SSL

Step 2: Edit the OpenSSL Configuration

- Open openssl.cfg in a text editor with administrative privileges.
- Add the following at the top of the file to enable dynamic engine loading:
 - openssl_conf = openssl_init
- Add the following at the end of the file to configure the PKCS#11 engine:

```
[openssl_init]
```

```
engines = engine_section
```

```
[engine_section]
```

```
pkcs11 = pkcs11_section
```

```
[pkcs11_section]
```

```
engine_id = pkcs11
```

```
dynamic_path = C:\\Program Files\\OpenSSL-Win64\\src\\pkcs11.dll
```

```
MODULE_PATH = C:\\Program
```

```
Files\\Utimaco\\SecurityServer\\Lib\\cs_pkcs11_R3.dll
```

```
init = 0
```

dynamic_path: Path to the OpenSC PKCS#11 Engine Plugin (pkcs11.dll) compiled in the prerequisites.

MODULE_PATH: Path to the Utimaco SecurityServer PKCS#11 Provider DLL.

Step 3: Verify OpenSSL Configuration and Connection

- Open a Command Prompt and run:
 - openssl engine pkcs11 -t
- Expected output confirms the PKCS#11 engine is available:

```
(pkcs11) PKCS#11 engine
```

```
[ available ]
```

4. Configure CodeSign Secure

CodeSign Secure requires configuration to connect to the Utimaco SecurityServer HSM for secure code signing operations. The **app-config.properties** file specifies the various details needed to successfully connect to Utimaco HSM.

Steps:

Step 1: Locate the app-config.properties File

- Navigate to the CertificateManagement folder inside the CodeSign Secure installation directory and locate the app-config.properties file, typically:

- C:\CodeSignSecure\src\CertificateManagement

Step 2: Update the HSM Details Fields

- Open app-config.properties in a text editor with administrative privileges.
- Update the following fields, replacing placeholders with your HSM connection details:

HSM_LIB_PATH_UTIMACO=<Path of cs_pkcs11_R3.dll file>

HSM_PIN_UTIMACO=<Login PIN for the Cryptographic User for a desired slot>

HSM_TOKEN_UTIMACO=<Slot Token Name>

HSM_SLOT_UTIMACO=<HSM Partition Slot Number>

- Save the file with the modified details.