Randtronics

DPM Key Manager

Integration Guide

CryptoServer

utimaco®

Imprint

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 working version

Date 06/10/2025

Status DRAFT

Document No. IG-2025-0008

Table of Contents

1 Introdcution

This document will guide you through the integration of a Utimaco CryptoServer (HSM, hardware security module) into Randtronics DPM easyKey, using the Utimaco JCE provider. This guide is targeted at version 1.4.x.x of DPM easyKey, for Windows and Linux.

For simplicity, paths are identified using forward slashes (/), when discussing both Windows and Linux OS installations. Windows-only or Windows-specific paths will continue to use back slases (\).

For guidance on the base installation and configuration of DPM easyKey, please see the installation media supplied with the application.

The integration steps below assume at least a basic knowledge of both the Utimaco SecurityServer software, and the DPM easyKey Tomcat web application.

This document is intended to be used as a quick guide in conjunction with Utimaco's primary documentation. For more detailed information on specific topics, please refer to the corresponding guides available.

Administration documentation will be found in the SecurityServer software installation, in the '{install}/ Documentation/Administration Guides' directory.

2 Requirements

2.1 Utimaco CryptoServer

For Windows, this document assumes an install location of `C:\Utimaco\CryptoServer`, and uses the SecurityServer-V4.21.x standard installation.

For Linux, this document assumes an install location of `/usr/opt/local/cs`.

This Integration Guide is a quick introduction and how-to, which should be used in conjunction with other Utimaco documentation found in the {install}/Documentation directories.

2.1.1 Setting up the environment

The DPM easyKey application will provide its own JCE configuration file, based on the input provided during the HSM configuration stage.

3 Configuration

3.1 Installing the Utimaco JCE Provider

The Utimaco JCE provider jar file is installed via the Windows installer for SecurityServer V4.21, if the JCE checkbox is checked when the API support page is displayed.

The Randtronics DPM easyKey will attach to the CryptoServer cluster via the CryptoServerJCE.jar, based on its own configuration file.

CryptoServerJCE.jar has one other dependency within the CryptoServer installation. If you have installed the SecurityServer software on one machine, but are running the Key Manager on another, you must copy CryptoServerJCE.jar and the platfrom dependent version of csadm (administration tool) to the Key Manager machine.

CryptoServerJCE.jar should be copied into the Key Manager's java classpath. The csadm tool should be copied from the SecurityServer installer .zip package directly, and into:

Windows, copy `{install}\Software\Windows\x86-64\Administration\csadm.exe` to `{dpmkm}\tomcat\binnative`.

Linux, copy `{install}/Software/Linux/x86-64/Administration/csadm` to `/usr/local/bin. In this case, ensure that /usr/local/bin` is configured in your $PATH environment variable.

Whether this is a single device or a cluster of devices will depend on the local configuration on the machine where the Key Manager is running.

3.2 Installing Randtronics DPM easyKey and Licensing

Install the Randtronics application using the product installers.

3.2.1 Windows OS

On Windows OS, the `.exe` will install the necessary packages and dependencies as needed, resulting in a Windows service with two HTTPS interfaces (using Tomcat).

This includes MySQL, if needed.

After the official installation is complete, copy the `{install}\Software\JCE\lib\CryptoServerJCE.jar file to {dpmkm}\Tomcat\Lib`.

After copying the jar file, open the Windows **Services** tool, and find the **DPM easyKey Web Server** service entry. Right click it, and select **Restart**.

3.2.2 Linux OS

On Linux, the installer application will place the necessary packages and dependencies as needed, resulting in a Tomcat service with the two HTTPS interfaces.

For Linux installs, MySQL must be manually pre-installed.

After the official installation is complete, copy the `{install}/Software/JCE/lib/CryptoServerJCE.jar file to {dpmkm}/Tomcat/Lib`.

On Linux, issue the following command to restart the Tomcat application:

>_console

```
$ service dpmeasykey restart
```

3.2.3 Post Install steps

The default ports for the interfaces discussed below are port 8543 (for management) and 5696 (for KMIP).

In a browser, navigate to:

https://127.0.0.1:8543/dpmkeymanager/login.jsp

The initial login is admin/admin.

On the CryptoServer side, using csadm or the CAT, create a user, for example 'dpmkm', with Cryptographic User permissions, and access to keys in the CXI_GROUP dpmkm:

>_Console

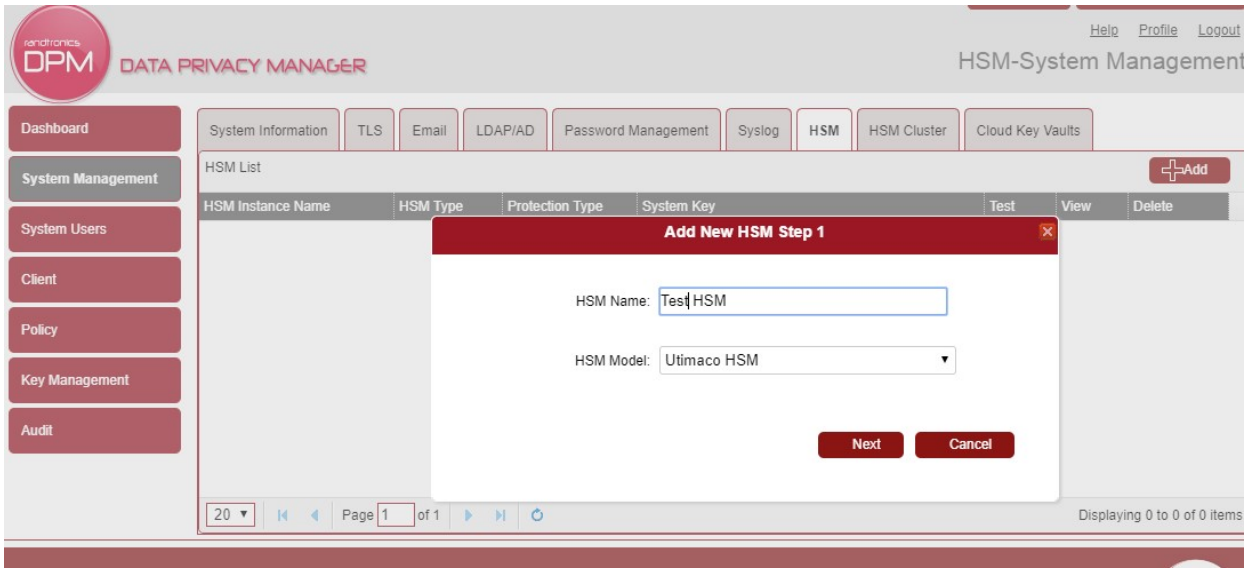
```
C:\> csadm Dev=<device> LogonSign=<user manager>,<credentials> ... \
AddUser=dpmkm,2{CXI_GROUP=dpmkm},hmacpwd,ask
```

Because the Utimaco tools parameters may change from release to release, you can get the parameters supported by your version of the tool, using the command `csadm help=AddUser`.

3.3 Adding support for the CryptoServer to DPM easyKey

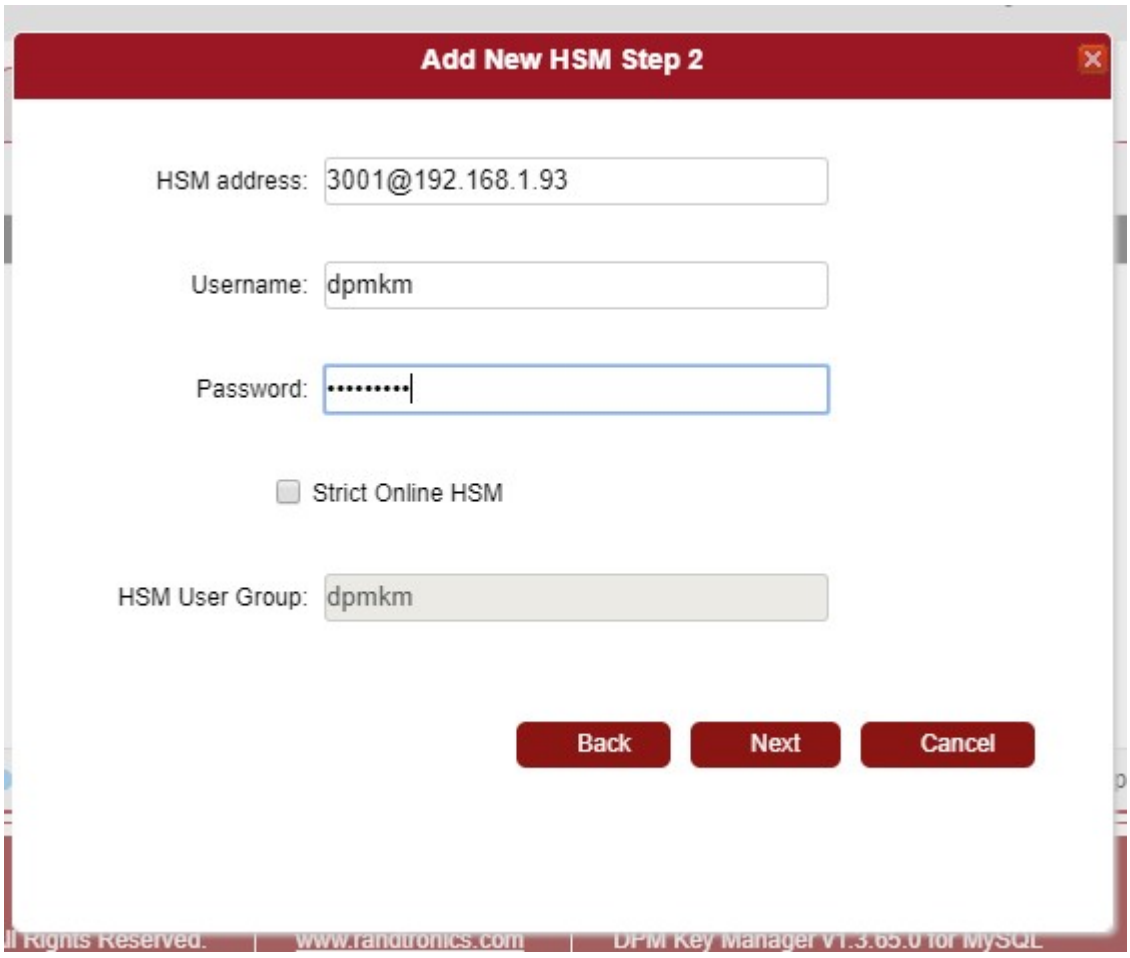
Log in to the application with administrator access. On the first login, you will need to provide a new admin password. Once re-logged in, navigate to the System Management tab (left side). Click on the **HSM** tab.

After the tab loads, click on the **[+ Add]** button. In the resulting dialog, name the HSM you are targeting. Select the Utimaco HSM from the dropdown. Click **Next**.

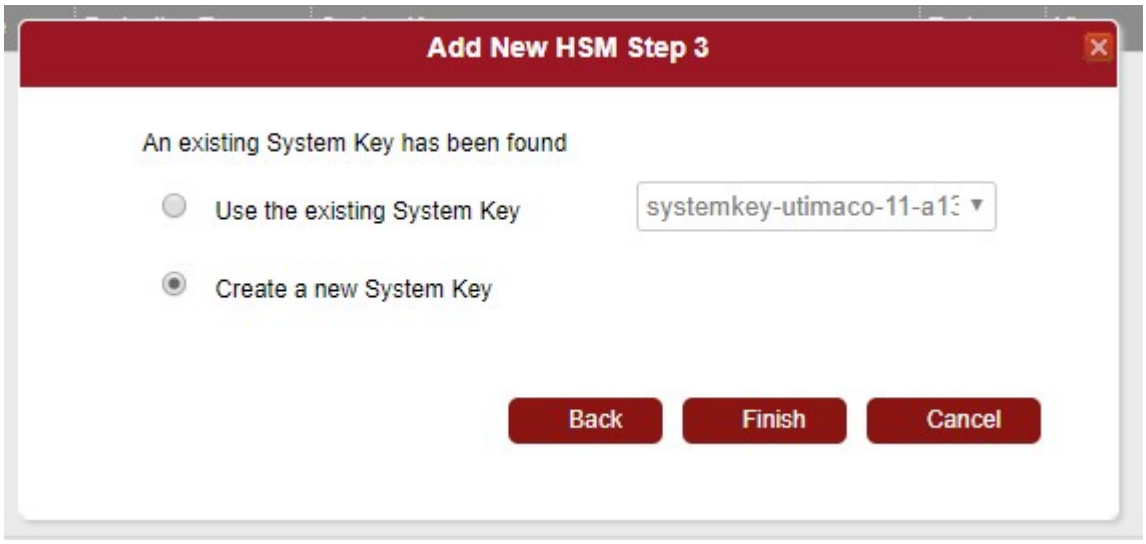


The next dialog asks for the connection string of the HSM. Enter the device's connection string, including the port number.

Enter the user name created above and the password. Leaving the 'Strict Online HSM' checkbox unset. Click **Next**.



Finally, choose a new system key (or select an existing), and click Next. This should finalize the connection and return you to the HSM List.



For more details please see Randtronics' 'DPM easyKey and Utimaco HSM Implementation Guide'.

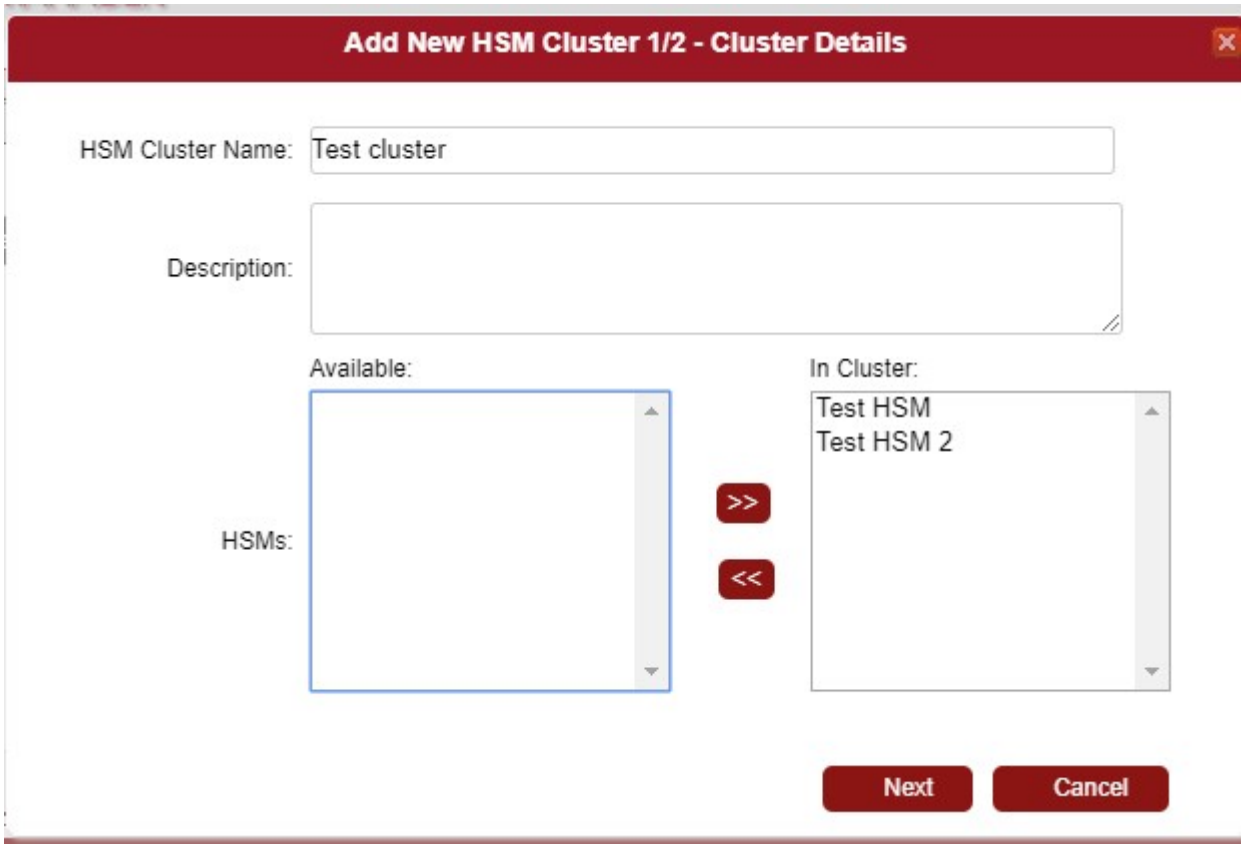
3.4 Adding support for a cluster of CryptoServers

DPM easyKey provides the ability to use multiple HSMs in a cluster.

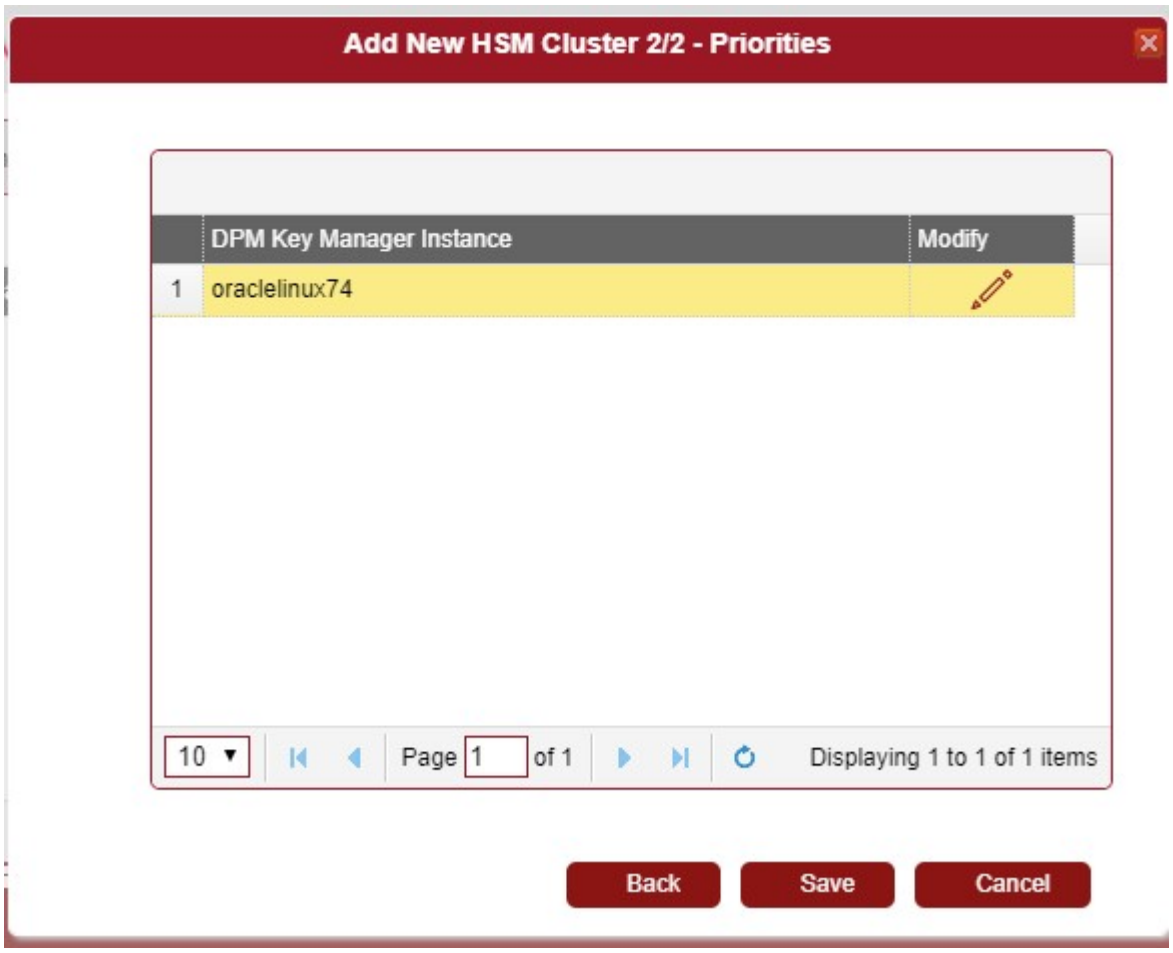
HSMs in the cluster are ordered based on a priority list. If a policy is configured to use a cluster of HSMs, then a key will be created using the first HSM from the cluster, based on the priority list. If the first HSM is not available then DPM will use the next in the list.

To create a cluster, navigate to the **System Management - HSM Cluster** tab.

After the tab loads, click on the **[+Add]** button. In the resulting dialog, name the HSM cluster. Select the target HSM from the **Available** list and move them to the list **In Cluster**. Click **Next**.

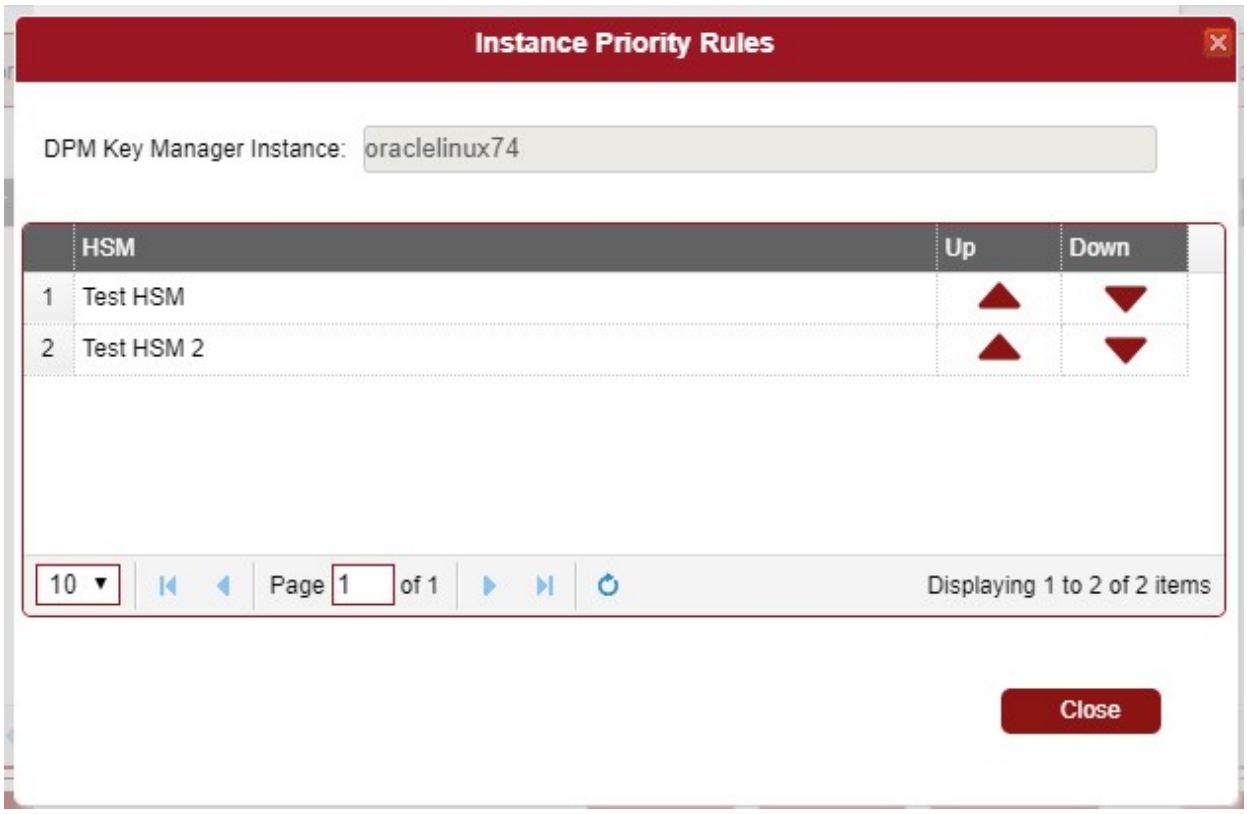


In the next dialog you can change default priority lists. There are separate priority lists for each DPM easyKey instance. This allows to target different HSMs based on a geographic location, country etc.



Click **Modify** for the desired DPM easyKey instance to change the priority list. Use **Up** and **Down** arrows to change priorities of the HSMs.

Click **Close** and **Save**.

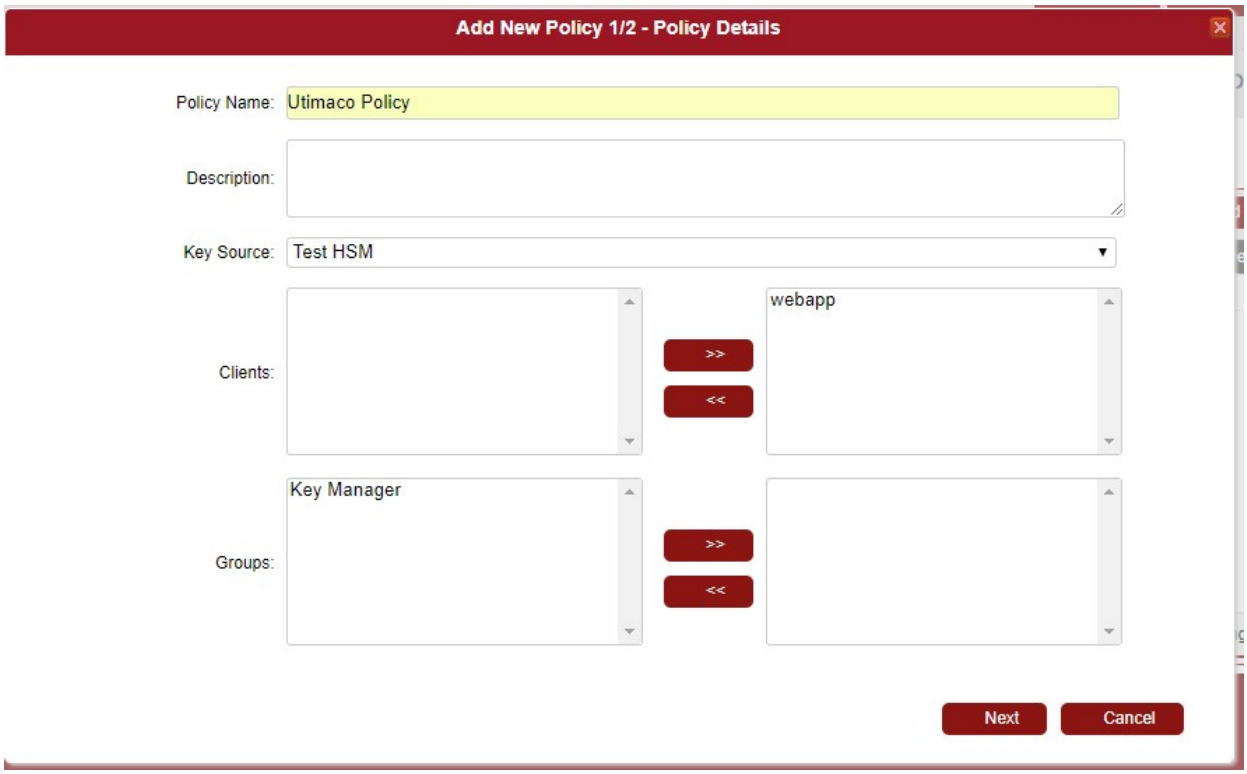


3.5 Using an HSM for key generation

To use an HSM for key generation, it should be configured in a Key policy for a client. Navigate to the Policy menu on the left.

Click **[+Add New Policy]**, and enter a policy name, then select a previously created HSM or HSM cluster in **Key Source**. Select a target client application and click **Next**.

On the next page add a key template and click **Save**.



When clients use this policy and the key template to create keys, key values will be generated by the HSM.
For more details please see 'DPM easyKey User Guide'.

4 Troubleshooting

4.1 Connection Problems

If you have problems connecting to the HSM, it is a good idea to make sure that your HSM is configured properly.

- Verify your HSM is running

  >_Console

  ```
  set CRYPTOSERVER=288@<ipaddr>
  csadm GetState
  ```

5 Further Information

This document forms a part of the information and support which is provided by Utimaco IS GmbH. All Utimaco CryptoServer documentation is available at the Utimaco IS GmbH website: https://hsm.utimaco.com, in the sup port portal (registration, login required).

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.