MyID Enterprise

Version 12.13

Entrust JASTK CA Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: INT2046-12.13.0-Enterprise

December 2024

Copyright

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document provides a step-by-step guide to the installation and configuration requirements to integrate the Entrust CA (Certification Authority) with MyID® using the Entrust Authority Security Administration Toolkit for Java (JASTK).

MyID has been tested with the following CA versions:

- Entrust 8.3.62.
- Entrust 10.0.40.
- Entrust 10.2.

Important: This support for JASTK supersedes MyID's integration with Entrust using the Entrust Administration Toolkit for C, as documented in the ***Entrust CA Integration Guide***. For assistance with migrating from the Entrust Administration Toolkit for C to the Entrust Authority Security Administration Toolkit for the Java Platform (JASTK), contact Intercede customer support quoting reference SUP-389.

You can use Entrust certificates in exactly the same way as any other certificate within MyID. For example. you can issue certificates to devices such as smart cards or VSCs, or to the local system as soft certificates.

MyID's integration with Entrust JASTK supports both RSA and ECC keys:

- For RSA keys, you can use certificates with 2048, 3072, and 4096 bit keys; 1024 bit keys are not currently supported with this CA.
- For ECC keys, you can use certificates with ECC NIST P256, P384, and P521 curves.

  Note: The Entrust Authority Security Toolkit for the Java Platform (ETJava) version 9 does not support ECC keys for escrow.

2 Configuration

This chapter contains instructions for configuring your Entrust system, including:

- Prerequisites for MyID's integration with Entrust, including the Java environment.

  See section *2.1*, *Prerequisites*.
- Creating the security officer and XAP profiles.

  See section *2.3*, *Create the MyID server profiles*.
- Setting up the link between MyID and Entrust.

  See section *2.4*, *Set up the MyID Entrust administration link*.
- Setting up key archival and recovery.

  See section *2.5*, *Key archival and recovery*.
- Setting up your directory.

  See section *2.6*, *LDAP configuration*.
- Setting up the configuration for the Entrust CA within the **Certificate Authorities** workflow.

  See section *2.7*, *Set up the MyID Entrust Certificate Authority*.
- Running the stored procedure to allow the mapping of certificate attributes.

  See section *2.8*, *Editing the CA policy in MyID*.
- Enabling certificate policies.

  See section *2.9*, *Enabling certificate policies*.
- Updating the details of an existing CA.

  See section *2.10*, *Updating the details of the CA*.
- Deleting a CA that is no longer required.

  See section *2.11*, *Deleting a CA*.
- Mapping certificate attributes for PIV systems.

  See section *2.12*, *Attribute mapping for PIV systems*.
- Information about ports required.

  See section *2.13*, *Ports required for Entrust*.
- Details of mandatory values.

  See section *2.14*, *Certificates with mandatory values*.
- Deactivating card authentication users.

  See section *2.15*, *Deactivation of card authentication users*.

2.1 Prerequisites

Before using the Entrust JASTK CA to issue certificates through MyID, you must install and configure the following software components on the MyID application server:

- Java.

  Entrust supports Java version 21 LTS; for example, Oracle Java SE Long Term Support (LTS) versions, or AdoptOpenJDK (LTS) version Hotspot. See the Entrust documentation for details.

  Note: This document uses the following for example file paths:

  ```
  C:\Program Files\Eclipse Adoptium\jdk-21.0.4.7-hotspot
  ```

  Your Java file paths may be different if you are using a different version of the JDK or the JRE. Use the appropriate paths based on your environment.
- Entrust Authority Security Administration Toolkit for Java (JASTK) version 10.0.3.8.
- Entrust Authority Security Toolkit for the Java Platform (ETJava) version 9.0.0.29.

You also need the following information and files to configure MyID to use the Entrust CA:

- Host address of the CA.
- Host port of the CA.
- DN of the CA (issuer of certificates).
- `Entrust.ini` file.
- Entrust Security officer profile file and password.
- An encryption certificate file and password.

  This is the certificate relating to the Encryption policy that is issued in Entrust to the security officer account. You may be able to convert the security officer's EPF profile file to a P12 file if you have an appropriate tool.

  This encryption certificate is required only if you are issuing archive certificates from your Entrust CA.
- The XAP server and port.

  XAP stands for XML Administration Protocol; this is used by Entrust for secure communication and management of digital certificates over HTTPS.
- The XAP profile file and password.

  This EPF contains the credentials for the XAP account.

  MyID requires access to the Entrust XAP web service. You can either extend the Entrust security officer profile to have the required permissions, or use a separate XAP profile.

2.1.1 Java Environment

To enable the Java Interface between MyID and the Entrust server to function correctly, all the `.JAR` files must be in the same location on the MyID application server. You have the following options:

- Copy the `etjastk.jar` file provided with the Entrust Authority Security Administration Toolkit for Java and the `enttoolkit.jar` file provided with the Entrust Authority Security Toolkit for the Java Platform to the directory containing the MyID Java component. If you have installed MyID in the default location, this is:

  `C:\Program Files\Intercede\MyID\Components\Java`

  or:

- Copy the MyID Java components to the directory containing the Entrust Authority Security Administration Toolkit for Java `.JAR` file.

  Once this has been done, open regedit and browse to the registry node:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJASTKConnector`

  If this registry entry does not exist, you must create it.

  Change the value of `JavaLocation` (which has type `String`) to the directory you have chosen to contain the `.JAR` files.

If you are using HSM-based credentials, you must also copy the following files from the Entrust Java Toolkit to the `System32` folder on the application server:

- `jnicapi_64.dll`
- `JNIPKCS11_64.dll`
- `UALJNI_64.dll`

2.1.1.1 Check the Path variable

You must check that the Path environment variable on the MyID application server contains both the location of the client `jvm.dll` file and its parent folder.

Important: If you update your version of Java, you must check the Path environment variable again, and update it if necessary.

1. Log on to the MyID application server as an account with administrative rights.
2. From the Windows Control panel, select **System**.
3. Click **Advanced system settings**.
4. Click **Environment Variables**.
5. From the list of **System variables**, select **Path**.
6. Click **Edit**.
7. Check that the full path of the folder containing the client `jvm.dll` file is included in the Path variable.

   For example:

   ```
   C:\Program Files\Eclipse Adoptium\jdk-21.0.4.7-hotspot\bin\server
   ```

   If this folder is not present in the path, add it.
8. Check that the path of the parent folder of the folder containing the client `jvm.dll` file is included in the Path variable.

   For example:

   ```
   C:\Program Files\Eclipse Adoptium\jdk-21.0.4.7-hotspot\bin
   ```

   If this folder is not present in the path, add it.

   Note: Make sure the paths are correct. If the paths are entered incorrectly, or are missing, you may experience errors, or you may experience a loss of functionality as the failure to find the `jvm.dll` file causes a silent failure.

   You must make sure that there are no spaces after the semicolons that delimit the entries in the path variable.

   For example:

   ```
   <Paths>;C:\Program Files\Eclipse Adoptium\jdk-21.0.4.7-
   hotspot\bin\server;C:\Program Files\Eclipse Adoptium\jdk-21.0.4.7-
   hotspot\bin;<More paths>
   ```
9. Click **OK** to save any changes you have made to the path.
10. Click **OK** to close **Environment Variables**.
11. Click **OK** to close **System Properties**.
12. Restart the server.

2.1.2 Issuing certificates to users who do not exist in the directory

If you want to issue certificates to users who do not exist in the directory, make sure you have set the `noUserInDirectory=1` setting for the certificate policies you want to issue.

If you do not set this, and attempt to issue a certificate to a user who does not exist in the directory, Entrust displays an error with the generic code `-1685`.

You can find this setting in the `master.certspec` file on the CA. See your CA documentation for the procedure for updating this file.

2.1.3 Certificate revocation list

The MyID application server must be able to communicate with the Certificate Revocation List (CRL) location. The CRL is checked for validity whenever MyID connects to the CA. If using a Microsoft ADS-backed CA, this is not the case by default for CRLs published to the directory. Ensure that your CRL publication is to a publicly accessible location.

2.1.4 Multiple Entrust digital identities with a single Luna SA HSM

It is possible for a toolkit application to support multiple Entrust digital identities concurrently with a single Luna SA HSM.

For more information, see the Entrust note reference TN7074.

One example could be two servers, Server1 and Server2 that require separate identities on the same Luna SA. In this case two partitions can be created on the Luna SA: PartitionA and PartitionB. PartitionA can then be assigned to Server1 and PartitionB can be assigned to Server2. When Server1 contacts the Luna SA through PKCS #11, PartitionA is exposed as a single slot visible on the Luna SA. Similarly Server2 sees one slot, as PartitionB is exposed to it. Each server based application can then create and log in to separate identities hosted on different partitions on the Luna SA.

In the case of multiple partitions assigned to a single client, for example, if Server1 has both PartitionA and PartitionB assigned to it:

The clients will see multiple slots. The ckdemo tool can be used to verify how many slots are exposed.

The Java based clients would just pick the desired slot and attempt to log in to the identity on that particular slot.

Entrust Authority Security Toolkit for the Java Platform (ETJava) would take the profile name that is specified and cycle through the slots until it finds the correct identity. The profile name (`.tkn` entry) should be the concatenation of the "Entrust Path" and "Entrust User" data blobs from the LunaSA with "`.tkn`" appended. A Windows based example could be something like:

```
d:\\test\\admintk\\luna_officer_wf.tkn
```

2.1.5 Certificate content

In some circumstances, it is possible that, for a given user, the contents of certificates are controlled by the Entrust policy; attributes may appear in certificates that you are not expecting. To prevent this, make sure that any unwanted extensions are explicitly blocked in the certificate policy configuration on the CA; use the SMA UI or another Entrust tool to enforce the Subject Alternative Name content.

2.1.6 User SID extensions

To set up your certificate authority to issue certificates with a user security identifier (user SID) extension for Windows authentication, you must configure the certificate template on the Entrust CA. See your Entrust documentation for details; the Entrust SMA User Guide provides instructions on how you configure a policy on the CA to accept the `objectsid`, and provides an example certificate type `ent_sid_keypair`.

In the **Certificate Authorities** workflow, you can edit the attributes for the policy to set the **User Security Identifier** attribute to have a **Dynamic** mapping to **User Security Identifier**; see section *2.9*, *Enabling certificate policies*.

For information on user SIDs, see the *Including user security identifiers in certificates* section in the ***Administration Guide***.

2.2 Differences with JASTK

Much of the configuration for JASTK is the same as the configuration for MyID's integration with Entrust using the Entrust Administration Toolkit for C, as documented in the ***Entrust CA Integration Guide***.

However, you must be aware of the following:

- You require the XAP (XML Administration Protocol) details of your CA, and must ensure the XAP port is open.

  See section *2.1*, *Prerequisites* and section *2.13*, *Ports required for Entrust*.
- You may require an additional XAP Entrust user profile in addition to the Admin EPF user profile.

  See section *2.3*, *Create the MyID server profiles*, section *2.4*, *Set up the MyID Entrust administration link*, and section *2.7*, *Set up the MyID Entrust Certificate Authority*.
- MyID's integration with Entrust JASTK supports both RSA and ECC keys.

  See section *1*, *Introduction*.
- Key sizes are determined on the CA and you cannot change them within MyID.

  See section *2.9*, *Enabling certificate policies*.
- The logging has changed significantly.

  See section *4.2*, *Entrust JASTK logging*.
- Deactivation of card authentication users is now a configuration option rather than registry controlled.

  See section *2.15*, *Deactivation of card authentication users*.
- The **Track Entrust distinguished name changes** option, which previously controlled whether MyID sent DN changes to Entrust when using the Entrust Administration Toolkit for C, is not relevant for Entrust JASTK. This option has now been removed from MyID.
- Attempting to issue certificates to users who do not exist in the directory now generates the generic error `-1685` instead of error `-2976` as previously.

  See section *2.1.2*, *Issuing certificates to users who do not exist in the directory*.
- The JASTK credentials that you use to authenticate to Entrust must have a different certificate type.

Previously, the admin credentials did not require the Admin Services User Management certificate type; JASTK requires this certificate type. If you are reusing credentials from an Entrust Administration Toolkit for C system, you must change the certificate type. You may need to collect new certificates, depending on the version of the Entrust CA and JASTK you are using.

2.3 Create the MyID server profiles

MyID requires a Security Officer level profile for administration of the Entrust system.

1. Within Entrust/RA, create a security officer and create a profile.
2. Right-click on the DN of the security officer and select **Add to Entrust** from the menu displayed.
3. The **User Properties** dialog box is displayed.
   a. On the **General** page check that:
      - **User role** is set to `Security Officer`
      - The **All groups** checkbox is selected
   b. Click **OK**
4. The **Create profile** dialog box is displayed.
   a. Enter a **Name** and a **Location** for the profile.
   b. Click **OK**.

You must also create a XAP user profile; see your Entrust documentation for details.

Note: You must issue the user credentials that you use to authenticate to Entrust (EPF files) with RSA key pairs and not ECC credentials.

2.3.1 Admin Services User Management certificate type

The JASTK credentials that you use to authenticate to Entrust must have the Admin Services User Management certificate type.

2.4 Set up the MyID Entrust administration link

1. Copy the `entrust.ini` file from your Entrust server to the MyID application server.

   This file must be configured for the type of smart card you are using.

   The file must also be configured for the HSM you are using, if appropriate. For example, for a Luna HSM, you must add the following to the `[Entrust Settings]` section:

   ```
   CryptokiV2LibraryNT=c:\Program Files\SafeNet\LunaClient\cryptoki.dll
   ```

   See your Entrust documentation for further information.

   Note: You must make sure that the FIPS value in the `entrust.ini` file is set to `0`. Failure to do this will usually result in an Entrust `error = -162` being reported when you try to test the connection.

   You must make sure the copy of the `entrust.ini` file on the MyID application server reflects your existing Entrust configuration. If the file changes on the Entrust server, you must copy it to the MyID server.

2. Copy the `.epf` or `.apf` files for the Security Officer and XAP profiles you created in section *2.3*, *Create the MyID server profiles*, to the MyID application server.

   Note: You must set write permissions for the MyID COM+ user for the profile files and their location, because it must be possible for Entrust to open these files with read/write access. The CA manages Entrust profiles and automatically updates them and when a key or certificate expires. You may see errors if this file is set to read only; for example, `-01055`.

2.5 Key archival and recovery

MyID can archive keys on the Entrust server, locally within MyID, or in the MyID SecureVault database – within the Certificate Authorities workflow, you can set the **Archive Keys** drop-down list to **None**, **Internal**, or **Secure Vault**; if you have MyID SecureVault installed, you can select **Secure Vault** to archive the keys in the MyID SecureVault database. For more information, see the *MyID SecureVault* section in the ***Administration Guide***.

if you configure your Entrust server for key archival, MyID displays either **Entrust** (for migrated policies) or **Entrust JASTK**; you cannot change this value.

Within Entrust, the client generation value may be true, false, or missing – you are advised not to leave the value as missing, but to set the value to true if you want to archive the keys within MyID, and false if you want to archive the keys within Entrust.

Note: If you recover a revoked archive certificate, and the certificate is configured in the credential profile for **Historic Only**, a new archive certificate is created on the CA; this is expected Entrust behavior, and MyID correctly ignores this certificate and recovers the old revoked archive certificate. This does not happen if the certificate is live, or if the certificate is configured in the credential profile to **Use existing**.

2.6 LDAP configuration

You must use the **Directory Management** workflow to configure a directory entry for the LDAP directory connected to the Entrust CA. Do not use anonymous access; you must provide the user DN and password for the directory.

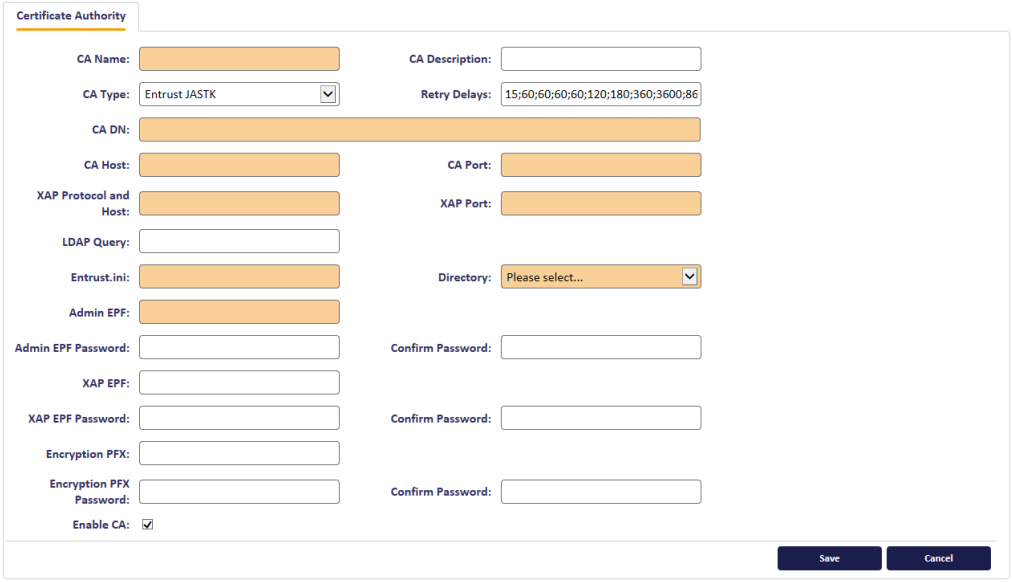
Note: MyID is configured for Active Directory by default; see section *3.2*, *Microsoft Active Directory*. If you want to use a different directory, or if MyID is using a different directory to the directory that Entrust is using, contact customer support, quoting reference SUP-195.

2.7 Set up the MyID Entrust Certificate Authority

Note: If you want to set up more than one Entrust CA within MyID, you may experience problems. For more information, contact customer support, quoting reference SUP-171.

To edit a Certificate Authority (CA):

1. From the **Configuration** category, select **Certificate Authorities**.
2. The **Certificate Authorities** workflow is displayed, with the **Select a CA** stage highlighted.
   - If an Entrust JASTK CA already exists, select it from the list and click **Edit**.
   - If an Entrust JASTKCA does not already exist, click **New**.
3. From the **CA Type** drop-down list, select **Entrust JASTK**.



Note: All of the fields with a colored background in the example are mandatory.

4. Set the following fields:
   - **CA Name** – Enter the name that you will use to identify the CA.
   - **CA Description** – Enter a description for the CA.
   - **CA Type** – Select **Entrust JASTK**.

- **Retry Delays** – A semi-colon separated list of elapsed times, in seconds.

  For example, `5;10;20` means:

  - If the first attempt to retrieve details from the CA fails, a second attempt will be made after a `5` second delay.
  - If this second attempt fails, the CA will be contacted again after `10` seconds.
  - Subsequent attempts will be made to retrieve information every `20` seconds, until a response is received.

  If you want to limit the number of retry attempts, enter `0` as the last number in the sequence.
- **CA DN** – Enter the DN (distinguished name) of the CA.

  You can obtain this value from the `CA Distinguished Name` item in the `[Entrust Settings]` section of the `entrust.ini` file.
- **CA Host** – Enter the DNS name or IP address of the Entrust server.
- **CA Port** – Enter the IP Port of the Entrust server. The default port number is `829`.

  The **CA Host** and **CA Port** values must match the settings for `Authority` in the `[Entrust Settings]` section of the `entrust.ini` file; for example:

  ```
  [Entrust Settings]

  Authority=myserver.example.com+829
  ```
- **XAP Protocol and Host** – Enter the address of the XAP host, including the protocol; for example:

  ```
  https://myserver.example.com
  ```
- **XAP Port** – Enter the port for the XP host. The default port number is `443`.

  The **XAP Protocol and Host** and **XAP Port** values must match the settings in the `[XAP Information]` section of the `entrust.ini` file; for example:

  ```
  [XAP Information]

  XAP=myserver.example.com+443
  ```

  Note: The `entrust.ini` file does not contain the protocol (http or https) but you must include it in the **XAP Protocol and Host** field.
- **LDAP Query** – Enter the query that MyID uses to find the Entrust LDAP entity.

  See section *3.1*, *Setting the LDAP query string* for details.
- **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.

  Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).
- **Directory** – Select the LDAP directory being used from the list available.
- **Admin EPF** – See section *2.7.1*, *Admin EPF* for details.

  Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).
- **Admin EPF Password** – Enter the password for the Admin EPF file.

- **XAP EPF** – Enter the full file path to the XAP epf file you created in section *2.3*, *Create the MyID server profiles*.

  Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

  The **XAP EPF** settings are optional; they may be required if the Admin EPF does not have the required credentials. See section *2.7.2*, *XAP EPF*.
- **XAP EPF Password** – Type and confirm the password for the XAP epf file.
- **Encryption PFX** – Enter the fully qualified path to the encryption certificate file. This can be a PFX or P12 file.

  important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

  Note: This encryption certificate is required only if you are going to be issuing archive certificates from your Entrust CA. If you do not want to issue archive certificates, you can leave this field blank.
- **Encryption PFX Password** – Enter the password used in conjunction with the encryption certificate file.

  The password is the same as the password associated with the EPF profile file that you used to generate the certificate file.
- Select **Enable CA** to make the policies available for issue.

5. Click **Save** to save these setting to the database.

Note: Changes made do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, then restart the **eCertificate** service.

MyID is now ready to issue certificates.

2.7.1 Admin EPF

The **Admin EPF** can either be the full file path to the epf file created in section *2.3*, *Create the MyID server profiles*, or a compound value representing the P11 library for your HSM, the slot serial number where the hardware based credential was created, and the name of that profile.

Note: The credential must be created with the Admin Services User Management certificate type.

Depending on what tools were used to create the hardware based credential, one or more files will have been created. You must copy those files to the MyID application server to a location with the same path as they were original generated.

Note: Contact Entrust for guidance on the appropriate tools for creating the hardware based credential; currently, Entrust suggest the PCU administration services utility.

An epf file can be copied anywhere – when it is a hardware based credential the copies of the files on the application server must match the location on the CA where they were created.

For example:

A hardware based credential was created into `c:\authdata\manager\epf` for a user HSM Officer. The profile for 'HSM Officer' was created (without a space) as HSMOfficer.

The files created, which will include one of more of `.apf/.arl/.cch/.crl/.pch/.xcc` must be copied to:

```
C:\authdata\manager\epf
```

on the MyID application server.

Within MyID, assuming your P11 DLL from your provider is `cryptoki.dll`, the Admin EPF value recorded in MyID would be:

```
<path to p11 dll>/SerialNumber|<ProfileName>.tkn
```

Note: There is no actual .tkn file at the location – the .tkn suffix is used to specify the name of the profile, not a filename.

Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

```
C:/Windows/System32/cryptoki.dll/123456789|HSMOfficer.tkn
```

Or if it is on the system path:

```
cryptoki.dll/123456789|HSMOfficer.tkn
```

Or if at the point of installation:

```
C:/Program Files/SafeNet/LunaClient/cryptoki.dll/123456789|HSMOfficer.tkn
```

Note: While you can use an HSM credential for both a system using the Entrust Administration Toolkit for C and JASTK, they must have their own HSM/slot/partition.

2.7.2 XAP EPF

MyID requires access to the Entrust XAP web service, and this service has specific requirements; see your Entrust documentation for details. You can either extend the Entrust security officer profile to have the required permissions, or use a separate XAP profile that has the required permissions.

If you do not specify a XAP EPF, MyID uses the Admin EPF to attempt to connect to the XAP service. If you specify a XAP EPF, MyID uses this XAP profile to connect to the XAP service.

If you are using HSM backed credentials, the XAP EPF has the same requirements as the Admin EPF described above.

2.8 Editing the CA policy in MyID

If you add a new CA or add a new policy to a CA, and want to enable the mapping of extended attributes, you must run the following stored procedure on the MyID database before you can edit the policy in MyID:

```
sp_SetEntrustCertExtensions_Jastk
```

Note: This is mandatory when setting up certificate policies on PIV systems – PIV requires the use of attribute mapping – but you can also use attribute mapping on non-PIV systems.

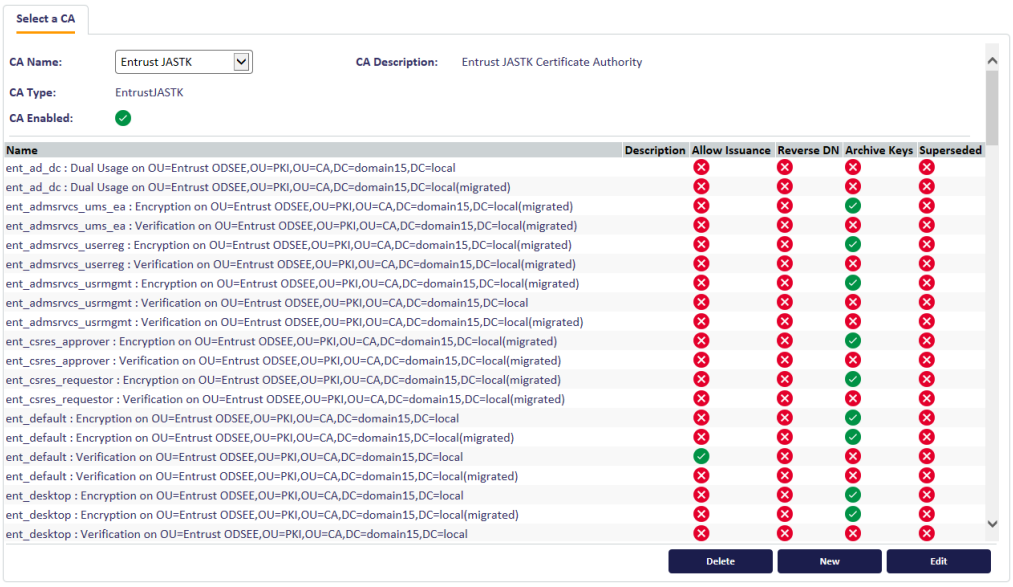
2.9 Enabling certificate policies

Important: You must make sure that all certificate types (on the CA) that you want to use as certificate policies in MyID have a specific certificate definition; that is, they have a specified user policy for that certificate type on the CA. You can change the user policy if required; MyID picks up the updated definition for the certificate policy when it next synchronizes with the CA.

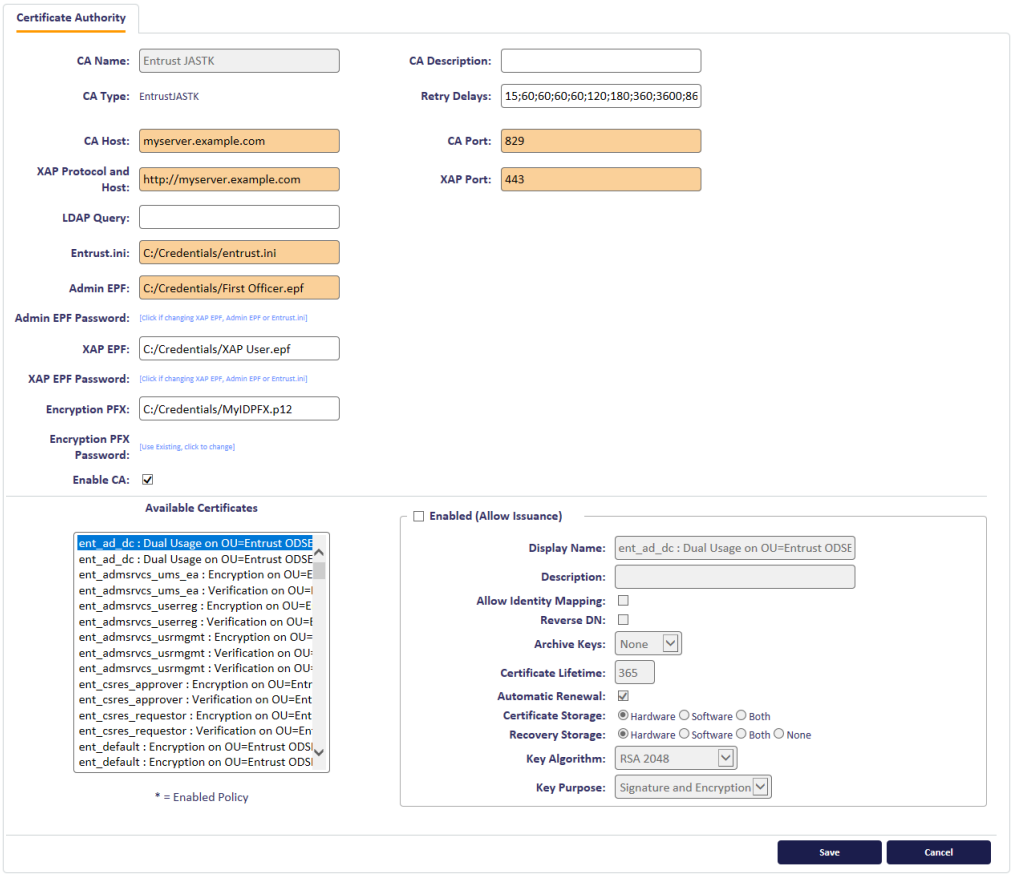
Note: You are recommended to set up your Entrust certificate policies to have a single key size and type.

Although all certificate policies are detected when you add the CA to MyID, they are all initially disabled. To enable them:

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.



3. Click **Edit**.



4. Make sure **Enable CA** is selected.
5. Select a certificate template you want to enable for issuance within MyID in the **Available Certificates** list.
6. Click the **Enabled (Allow Issuance)** checkbox.
7. Set the options for the policy:
   - **Display Name** – the name used to refer to the policy.
   - **Description** – a description of the policy.
   - **Allow Identity Mapping** – used for additional identities. See the *Additional identities* section in the ***Administration Guide*** for details.
   - **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed.

     Note: MyID does not recognize this option when using the **Issue Card** workflow to issue a card.
   - **Archive Keys** – select whether the keys should be archived.

     If you have set up the keys to be archived in Entrust, this option displays either **Entrust** (for migrated policies) or **Entrust JASTK**, and you cannot change the option.

     Otherwise, you can select one of the following values from the drop-down list:
     - **None** – the certificates are not archived.
     - **Internal** – the certificates are archived in the MyID database.
     - **Secure Vault** – if you have MyID SecureVault installed, you can select **Secure Vault** to archive the keys in the MyID SecureVault database. For more information, see the *MyID SecureVault* section in the ***Administration Guide***.
   - **Certificate Lifetime** – the life in days of the certificate. You can request a certificate from one day up to the maximum imposed by the CA. For example, type `365` to request one-year certificates.

     Note: The default certificate lifetime value in MyID is 365 days. The default in Entrust is 36 months; if you want to configure MyID to match the Entrust default, enter 1095 days.
   - **Automatic Renewal** – select this option if the certificate is automatically renewed when it expires.
   - **Certificate Storage** – select one of the following:
     - **Hardware** – the certificate can be issued to cards.
     - **Software** – the certificate can be issued as a soft certificate.
     - **Both** – the certificate can be issued either to a card to as a soft certificate.
   - **Recovery Storage** – select one of the following:
     - **Hardware** – the certificate can be recovered to cards.
     - **Software** – the certificate can be recovered as a soft certificate.
     - **Both** – the certificate can be recovered either to cards or to a soft certificate.

- **None** – allows you to prevent a certificate from being issued as a historic certificate, even if the **Archive Keys** option is set.

  If the **Certificate Storage** option is set to **Both**, the certificate can be issued to multiple credentials as a shared live certificate, but cannot be recovered as a historic certificate.

- Additional options for storage:

  If you select **Software** or **Both** for the **Certificate Storage**, or **Software**, **Both**, or **None** for the **Recovery Storage**, set the following options:

  - **CSP Name** – select the name of the cryptographic service provider for the certificate. This option affects software certificates issued or recovered to local store for Windows PCs.

    The CSP you select determines what type of certificate templates you can use. For example, if you want to use a 2048-bit key algorithm, you cannot select the Microsoft Base Cryptographic Provider; you must select the Microsoft Enhanced Cryptographic Provider. See your Microsoft documentation for details.

  - **Requires Validation** – select this option if the certificate requires validation.

  - **Private Key Exportable** – when a software certificate is issued to local store, create the private key as exportable. This allows the user to export the private key as a PFX at any point after issuance.

    It is recommended that private keys are set as non-exportable for maximum security.

    Note: This setting affects only private keys for software certificates – private keys for smart cards are never exportable.

    Note: By default, when MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2. However, some Operating Systems do not support this modern security standard, which creates a problem when importing the certificates onto these; for example, any Apple OS (macOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709. If you want to import software certificates onto an OS that does support not the encryption of PFX files using AES256/SHA2, you must set the **Use SHA1 encryption for certificates issued as PFX files** option in the **Server** tab of the **Security Settings** workflow to `Yes`.

  - **User Protected** – allows a user to set a password to protect the certificate when they issue or recover it to their local store.

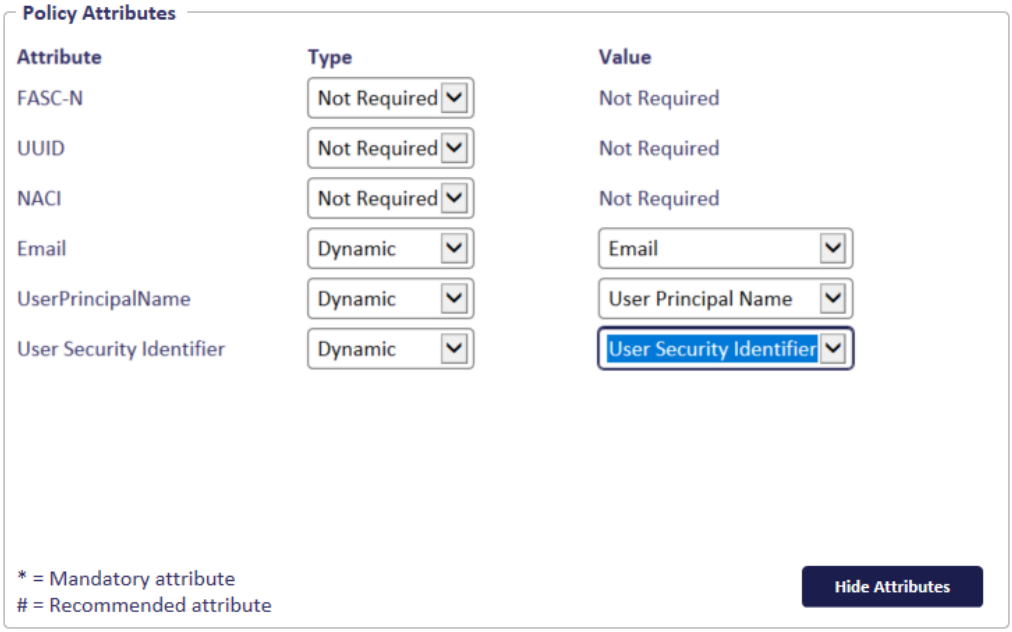
    This means that whenever they want to make use of the soft certificate, they will be prompted for a password before they are allowed to use it. This is a CSP feature that is enabled when you set this option, and affects only software certificates that are issued or recovered to local store for Windows PCs.

- **Key Algorithm** – you must configure the key algorithm on the Entrust server. This option is display-only within MyID.

- **Key Purpose** – you must configure the key purpose on the Entrust server. This option is display-only within MyID. The key purpose can be one of the following:
  - **Signature** – the key can be used for signing only.
  - **Signature and Encryption** – the key can be used for either signing or encryption.

  Note: The **Key Purpose** option has an effect only where the device being issued supports the feature. PIV cards do not support this feature, while smart cards issued with minidrivers and software certificates issued to local store for Windows PCs do support this feature.

8. If you need to edit the policy attributes, click **Edit Attributes**.



   a. For each attribute, select one of the following options from the **Type** list:
      - **Not Required** – the attribute is not needed.
      - **Dynamic** – select a mapping from the **Value** list to match to this attribute.
      - **Static** – type a value in the **Value** box.

   b. Click **Hide Attributes**.

   For information on mapping attributes for PIV systems, see section *2.12*, *Attribute mapping for PIV systems*.

   Note: MyID may not override the settings of the CA. You need to obtain the correct settings from the administrator of your CA.

9. Click **Save**.

Note: Changes made to certificate profiles do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, then restart the **eCertificate** service.

2.9.1 Controlling certificate lifetimes

For PIV compliance and the desire to enable finer control over the issuance of certificates, MyID provides a certificate-based operation setting to constrain certificate lifetimes to the lifetime of the credential. That setting means certificate requests potentially, and by default are, restricted to lifetimes with their associated credential.

You can configure MyID to use the CA default lifetimes instead; typically, this is 36 months. MyID stores a representative value in the `EnProfileTemplates` table in the MyID database; however, individual CA instances may vary. When you enable this option, MyID is given whatever that particular instance is using for its 'user default key update policy'.

To set up MyID to use the CA default lifetimes:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Certificates** tab.
3. Set the following option:
   - **Use Entrust default key update policy**

     Set this value to `Yes` to use the CA's default lifetimes.

     Set this value to `No` to constrain certificate lifetimes to the lifetime of the credential.
4. Click **Save changes**.

Entrust maintains a single value for all users however on a user by user basis, and therefore their certificate requests can have a specific or the default policy in place.

2.9.1.1 Effect on escrowed encryption certificates of allowing the CA to control lifetimes

If you have set the **Use Entrust default key update policy** option to `Yes`, and the CA is in control of certificate lifetimes, the behavior of Entrust when issuing encryption certificates is different. When MyID controls the lifetimes, when you issue an encryption certificate, Entrust always issues a new certificate. However, when Entrust controls the lifetimes, it issues a new encryption certificate only if there is not an existing escrowed encryption certificate; if there is an existing escrowed active encryption certificate, Entrust issues a copy instead.

Note, however, that if the existing certificate is expiring, Entrust issues a new certificate rather than recovering a copy.

2.9.2 Forcing the issuance of new escrow certificates

To force Entrust to issue new escrow certificates:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Certificates** tab.
3. Set the following option:
   - **Entrust force new escrow**

     When this option is set to `Yes`, if Entrust returns an existing escrow certificate in response to a request for a new certificate, MyID revokes the certificate and requests the new certificate again.

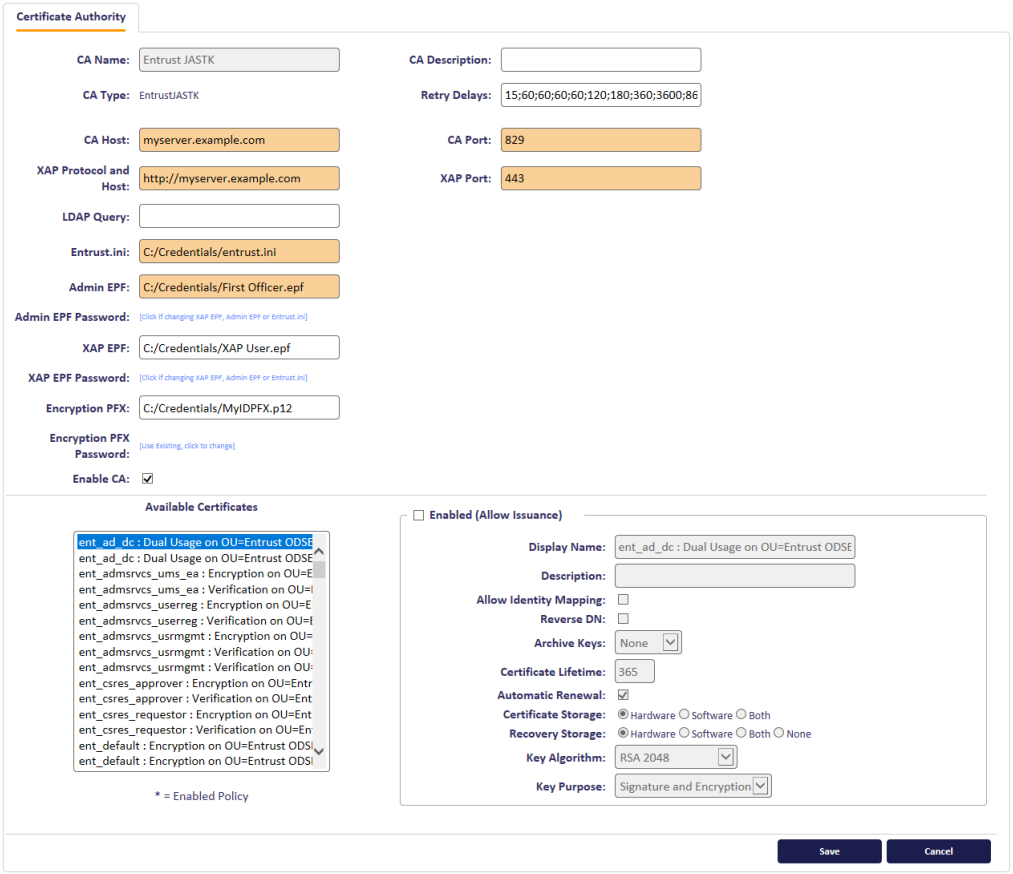
     The default is `No`.
4. Click **Save changes**.

Note: Setting this option returns MyID to its previous behavior; you are recommended to keep this option at the default `No` for most systems, and set this option to `Yes` only if directed to by Intercede.

2.10 Updating the details of the CA

You can edit the configuration for the CA.

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.
3. Click **Edit**.



4. Make sure **Enable CA** is selected.
5. You can edit the following:
   - **CA Host** – Enter the DNS name or IP address of the Entrust server.
   - **CA Port** – Enter the IP Port of the Entrust server. The default port number is `829`.

     You can confirm the port number from the `CMPListen` item in the `[Comms]` section of the `entmgr.ini` file.
   - **LDAP Query** – Enter the query that MyID uses to find the Entrust LDAP entity.

     See section *3.1*, *Setting the LDAP query string* for details.
   - **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.
   - **Admin EPF** – See section *2.7.1*, *Admin EPF* for details.
   - **XAP EPF** – See section *2.7.2*, *XAP EPF* for details.

Note: If you change the **LDAP Query**, **Entrust.ini**, **Admin EPF**, or **XAP EPF**, you must re-enter the **Admin EPF Password** and **XAP EPF Password**; the password fields become visible automatically. Otherwise, if you need to change the passwords, click the link to display the password fields.

- **Encryption PFX** – Enter the fully qualified path to the signing PFX file.

  Note: If the **Encryption PFX Password** has not changed, you do not need to re-enter it. If the password has changed, click the link to display the password fields.

6. Click **Save**.

2.11 Deleting a CA

You can delete a CA from the list of available CAs if you no longer need to be able to work with it, or if you created it in error.

See the *Deleting a CA* section in the ***Administration Guide*** for details.

2.12 Attribute mapping for PIV systems

For PIV systems, you must set up the attributes of the PIV certificate policies to have specific dynamic mappings.

Note: The FASC-N mapping is required for standard PIV cards, but is not permitted for PIV-I cards. The PIV Card Authentication certificate policy *must not* contain a mapping for Email.

2.12.1 Example attribute mapping for PIV systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	User Principal Name	Not Required
PIV Card Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.12.2 Example attribute mapping for PIV-I systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	Not Required	UUID (ASCII)	Not Required	User Principal Name	Not Required
PIV Card Authentication	Not Required	UUID (ASCII)	Not Required	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.12.3 Editing the attribute mappings

To edit the attribute mapping:

1. Within the **Certificate Authorities** workflow, select an enabled certificate policy.
2. Click **Edit Attributes**.
3. For each attribute, select one of the following options from the **Type** list:
   - **Not Required** – the attribute is not needed.
   - **Dynamic** – select a mapping from the **Value** list to match to this attribute.
   - **Static** – type a value in the **Value** box.
4. Click **Save**.

2.13 Ports required for Entrust

You must configure your firewall so that the ports specified in the `entrust.ini` file are open between the client and the CA or LDAP.

The `entrust.ini` file refers to the following ports:

Entrust.ini reference	Port	Needed by the client?
Authority	829	Yes
Manager	709	No
Server	389†	Yes
ASHServer	710	Yes
XAP	443	Yes

†Where the LDAP port is variable between installations, 1389 and 389 are used locally depending on LDAP used – ODSEE or ADS.

2.14 Certificates with mandatory values

You can configure your certificate policies to have mandatory values; for example, on PIV systems, you can configure your certificate policies to make the NACI value mandatory (the `piv_interim` attribute, known as `interim_indicator` in Entrust). This is typically required for the PIV Authentication and PIV Card Authentication certificates. When MyID adds the user to Entrust, it includes the user's NACI value.

Note: This is relevant for PIV systems only. Users in MyID Enterprise systems do not have NACI values.

MyID makes sure to provide the user's captured NACI/`interim_indicator` value when it adds the user to Entrust.

Previously, you were recommended to use an optional setting, which meant that while MyID would still encode the value for certificate submission, it did not need to provide it at the point of adding the user; typically the Card Authentication DN where MyID creates a new user for each issuance.

MyID now provides the captured value both as part of the user addition and the submission, whether it is `TRUE` for incomplete or `FALSE` for NACI complete at both steps.

For most deployments that use the existing recommended optional `interim_indicator` value, this change makes no difference. For sites that want to use the now-deprecated NACI value in Card Authentication certificates, you can now use a mandatory `interim_indicator`.

If the MyID administrator does not configure a user attribute for use in NACI submissions, the certificate issuance will still fail and report an error similar to:

```
The variable Interim Indicator: (interim indicator) does not have a value defined.
```

The change here is merely to provide it earlier in the Entrust user creation sequence, not create a value where none is present.

Note: If the CA being used has optional NACI configured, for a user without a NACI set and depending on the order that the certificates are issued, you may see the Card Authentication or PIV Authentication certificate be successfully issued before the issuance process fails and the certificates are then subsequently revoked.

2.15 Deactivation of card authentication users

PIV Card Authentication certificates are usually issued to a different subject DN than other certificates, which is formed from the card FASC-N or GUID. As a result, the Entrust PKI creates an additional user account for this subject. The MyID Entrust PKI connector can deactivate this additional account when card authentication certificates are revoked.

If you want to deactivate the additional account, set the **Deactivate Card Auth user in Entrust** option (on the **Certificates** page of the **Operation Settings** workflow) to `Yes`. The account is deactivated if:

- The certificate being revoked was issued to the PIV Card Authentication container (5FC101).
- The certificate was issued to a subject that is not the user's main Distinguished Name – the value is normalized to take whitespace into account.

To handle card reprovision events, if MyID attempts to issue a new certificate to an Entrust user who is deactivated, the user is reactivated.

3 Using directory services

The Entrust CA stores certificate policy information in the directory as an attribute of the CA entry. MyID has to be able to read this information to get the policy information and certificates that are available for issuance by MyID.

As the Entrust CA stores this information as an attribute of the CA object in the directory, MyID searches for the LDAP entity given the DN of the CA and the `objectClass` of `entrustCA`.

3.1 Setting the LDAP query string

In some installations it may be found that the LDAP directory server being used will not support the default query:

```
(objectClass=entrustCA)
```

For example, it may be `CA` or something similar; for Active Directory, the query should be:

```
(objectclass=certificationAuthority)
```

See your *Security Manager Directory Configuration Guide* (provided by Entrust) for details.

To allow for this, you can specify the query in the **LDAP Query** field of the **Certificate Authorities** workflow when you set up the CA in MyID.

3.2 Microsoft Active Directory

For a successful installation of the MyID system and the Entrust CA and Microsoft Active Directory Server there are some special requirements.

- The connection to the directory must be authenticated. When configuring the Directory connection within MyID, be sure to specify a username and password and the host and port information for the server. You cannot use an anonymous connection.
- The user specified for the directory configuration must be a member of the Entrust Security Administrators group on the Active Directory Server. You will need to have an administrator of the directory server do this.
- The LDAP root DN needs to be set as in the following format:

```
cn=AIA,cn=Public Key Services,cn=Services,cn=Configuration
```

followed by your particular domain information.

For example:

```
cn=AIA,cn=Public Key
Services,cn=Services,cn=Configuration,dc=mydomain,dc=co,dc=uk
```

3.3 Updating Entrust DN changes

You cannot trigger updates for Entrust DN changes on MyID Enterprise systems. Using the **Track Entrust distinguished name changes** option on the **LDAP** tab of the **Operation Settings** workflow is *not* supported using Entrust JASTK. Previously, this option was added for MyID Enterprise systems when using the Entrust Administration Toolkit for C, but has now been removed, and is not relevant for Entrust JASTK on either PIV or Enterprise systems. Updating Entrust DN changes *is* supported on MyID PIV systems, but does not use this option.

3.4 DN order

Entrust controls the order of the elements of the DN. Your Entrust system may have a different server-side configuration, but by default:

- The DN order may be different between archived and non-archived certificates. If you find that CA-generated certificates are issuing to different users, you are recommended to try setting the **Reverse DN** option for either the non-archived or the archived certificate policy. This behavior may be different across different installations of Entrust.
- When issuing internally archived Entrust certificates, the DN is always CN first regardless of the source DN format or the state of the **Reverse DN** flag.
- The ordering of DN elements within a certificate request is not always implemented consistently. The issuance of credentials where keys are generated on mobile devices implements ordering differently to requests generated on cards or by MyID for archived certificates.

  Therefore, if you need to keep a consistent DN order across issued certificates, you are recommended to use an independent non-archived certificate policy for mobile credentials, and set the **Reverse DN** option for this policy to the opposite of the value used for archived certificates and card-issued non-archived certificates.

3.4.1 Reversing user DNs

You must align Entrust user DN ordering and MyID DN ordering (where possible) through the use of the **Reverse DN** setting for each Entrust certificate policy in the CA workflow. A typical user's ordering reflects the CA's own DN ordering.

For example, for a CA whose DN is in the form:

```
ou=MyEntrustCA,ou=PKI,ou=CA,dc=mydomain,dc=local
```

Users (known to the CA) would be in the form:

```
cn=Arthur Alpha,ou=MyEntrustCA,ou=PKI,ou=CA,dc=mydomain,dc=local
```

However, for PIV issuance, where the form is:

```
dc=local, dc=mydomain, ou=CA, ou=PKI, ou=MyEntrustCA, cn=Arthur Alpha
```

Or in the alternative `noUserInDirectory` case:

```
C=US, o=U.S. Government, ou=Department of Administration, cn=Arthur Alpha
```

You must set the **Reverse DN** flag to true.

Note: MyID does not recognize this option when using the **Issue Card** workflow to issue a card.

4 Troubleshooting

This chapter contains information about:

- Error messages that may appear when using Entrust.

  See section *4.1*, *Troubleshooting error messages*.
- Configuring logging for the Entrust connector.

  See section *4.2*, *Entrust JASTK logging*.
- Setting up auditing.

  See section *4.3*, *Auditing*.

4.1 Troubleshooting error messages

- **CA reporting error -142**

  This error, which presents as "INI file mismatch", may be caused by DNS lookup problems. Make sure that all servers have fully resolvable addresses and do not have DNS issues.

- **CA reporting error -162**

  You must make sure that the FIPS value in the `entrust.ini` file is set to `0`. Failure to do this will usually result in an `Entrust error = -162` being reported when you try to test the connection.

- **CA reporting error -2187**

  This error may be caused by incorrect mapping in the certificate attributes; for example, if you have mapped the **FASC-N** attribute to **FASC-N (ASCII)** instead of **FASC-N (Hex)**.

- **CA reporting error -2921**

  This CA error – `THE SIGNING/ENCRYPTION EXPIRATION DATE EXCEEDS THE LONGEST ALLOWED CERTIFICATE LIFETIME` – may occur if you have configured MyID to request a date that the CA cannot honor; that is, the CA's own certificate expires before the user certificate end date that you have requested.

  If you see an error with this code, you must reduce the credential profile or certificate lifetime to within a range that your CA can support. See your CA administrator for details of your CA's limits.

- **CA reporting error "The variable Interim Indicator: (interim indicator) does not have a value defined."**

  If you are working in a PIV environment, and your CA reports an error similar to:

  ```
  The variable Interim Indicator: (interim indicator) does not have a value defined.
  ```

  you may need to update your `certspec` to remove the rule for `interim_indicator`.

  This error may also be caused (on a customized MyID system that passes Entrust user roles to the CA when requesting a certificate) by a mismatch between the user roles listed on the MyID system and in the Entrust CA. Make sure that the lists on the CA match the lists in MyID. Check the Entrust logs for more information on what might be causing this error.

- **CA reporting error -32712**

  This CA error – `GIVEN TIME VALUE IS NOT VALID` – relates to invalid time values that have previously occurred in situations relating to an overflow in the epoch calculation. If you see an error with this code, contact Intercede customer support, providing as much logging detail as possible.

- **CA reporting error -01055**

  This CA error – `UNABLE TO LOCK THE PROFILE FOR UPDATING` – relates to problems loading the Entrust EPF. If you see this error in your Entrust logs, try giving the MyID COM+ user local administrator privileges.

- **CA reporting error "Elliptic Curve keys (EC keys) are not supported by the CardMS API (168005)"**

You have attempted to issue certificates using ECC keys and escrow; the Entrust Authority Security Toolkit for the Java Platform (ETJava) version 9 does not support ECC keys for escrow.

- **MyID reporting "Card Server Error During Process"**

  After upgrading MyID, if you see an error similar to:

  ```
  Card Server Error During Process
  ```

  when attempting to issue a certificate, with details similar to:

  ```
  BOL COM catch handler Function : ProcessAPDUCommand, catch handler.
  Error : Unspecified error An error occurred inside
  PivCardServer::ProcessCommand Error: 0x80004005 Unspecified error
  Unable to locate java method GetArchCert Unable to locate java method
  GetArchCert ------------------------ Exception raised in function:
  JavaEnvironment::GetMethodID In file JavaEnvironment.cpp at line 132 --
  ---------------------- Exception raised in function:
  JavaAccessor::getArchivedCertificate In file JavaAccessor.cpp at line
  67 In object EntrustJTKConnector.KeyStore.1
  ```

  this may have been caused by an issue during the upgrade installation process that prevented the `EntrustJTKConnector.jar` file from being replaced. As a workaround, you can copy the `EntrustJTKConnector.jar` file from another system, or you can raise a support case with Intercede to identify the cause – to do so, you must provide the `TestReports` folder from the MyID Installation Assistant and quote reference SUP-376.

- **The JASTK credential does not have the Admin Services User Management certificate type**

  If you see an error similar to:

  ```
  INFO: com.entrust.adminservices.toolkit.internal.xap.XAPException:
  (AtkXap.XAP.1003) A required policy oid is missing from the
  certificate. The XAP Server profile and the client profile should be
  created with the correct certificate types. The missing oid was
  2.16.840.1.114027.10.4
  ```

  This may be caused by the JASTK credential not having the Admin Services User Management certificate type.

  Note: If you are using an HSM, this issue may present as an error similar to:

  ```
  Aug 15, 2024 1:35:06 PM com.intercede.pki.entrust.jastk.Utility
  getHSMProfileReader
  INFO: Found SerialNumber (1393032467824) Slot (0) SlotID (3)
  Aug 15, 2024 1:35:11 PM com.intercede.pki.entrust.jastk.Utility
  getThrowable
  WARNING: Root com.entrust.toolkit.exceptions.UserFatalException: The
  'Keys' section has been tampered
  ```

- **Defining an extension for a policy that is not configured for the policy type**

  If you see errors similar to:

  ```
  Sept 02, 2024 3:25:47 PM
  com.intercede.pki.entrust.jastk.CertificateRequest submit
  ```

```
WARNING: com.entrust.adminservices.toolkit.internal.xap.XAPException:
(AtkApi.main.3008) Unable to modify the properties of user cn=Alise
Rice,ou=Department of Education,ou=PIV,dc=domain25,dc=local. Caused by:
com.entrust.adminservices.toolkit.internal.xap.XAPException:
(AtkApi.main.1046) The variable id_vettingdate_var is not a valid
variable for the certificate type ent_desktop.

Sept 02, 2024 3:25:47 PM com.intercede.pki.entrust.jastk.Utility
getStackTrace

INFO: com.entrust.adminservices.toolkit.internal.xap.XAPException:
(AtkApi.main.3008) Unable to modify the properties of user cn=Alise
Rice,ou=Department of Education,ou=PIV,dc=domain25,dc=local. Caused by:
com.entrust.adminservices.toolkit.internal.xap.XAPException:
(AtkApi.main.1046) The variable id_vettingdate_var is not a valid
variable for the certificate type ent_desktop.
```

This may be caused by defining an extension for a certificate policy that is not configured for the policy type. Make sure that you have defined the correct extensions for the policy.

4.2 Entrust JASTK logging

This section contains information on enabling logging for the Entrust JASTK components.

Important: Disable the logging when you have completed diagnosing the issues, as the log files may become very large.

4.2.1 Setting up logging in the connector properties file

You can configure the log level, log file, and log format for MyID's logging of the JASTK connector using the properties file; by default, this file is:

`C:\Program Files\Intercede\MyID\Components\Java\jastkconnector.properties`

Use a text editor to edit the file. You can set edit the following lines:

- `.level= OFF`

  The global setting for log level.

  Note: If you set the `.level` value to anything other than `OFF`, but keep the `java.util.logging.FileHandler.level` set to `OFF`, the log file is created, but nothing is written to it.

- `java.util.logging.FileHandler.pattern = c:/logs/myid_%u_%g.log`

  The location and filename to use for the log.

  Where:

  - `%u` is a unique number to resolve conflicts between simultaneous Java processes.
  - `%g` is the generation number to distinguish between rotating logs.

- `java.util.logging.FileHandler.limit = 10000000`

  The maximum size of the file, in bytes. If this is `0`, there is no limit. Logs larger than limit roll over to the next log file.

- `java.util.logging.FileHandler.count = 1`

  The number of log files to use in the log file rotation.

- `java.util.logging.FileHandler.level = OFF`

  The level of logging you want. Specify one of the following, from least to most output:

  - `OFF`
  - `SEVERE`
  - `WARNING`
  - `INFO`
  - `CONFIG`
  - `FINE`
  - `FINER`
  - `FINEST`
  - `ALL`

- `#java.util.logging.SimpleFormatter.format=%4$s: %5$s [%1$tc]%n`

  Uncomment this line (`#`) if you want to specify the format for the log entries. You can use the following codes:

  - `%0$` – format – the format string.
  - `%1$` – date – the date and time of the log message.
  - `%2$` – source – a string representing the caller, if available; otherwise, the logger's name.
  - `%3$` – logger – the logger's name.
  - `%4$` – level – the log level.
  - `%5$` – message – the formatted log message.
  - `%6$` – thrown – the thrown error including the backtrace, if any.

  For dates, you can use Java `printf` formatting; for example:

  - `%1$tc`

    Tue Mar 22 13:11:31 PDT 2024
  - `%1$tb %1$td`

    Mar 22
  - `%1$tl:%1$tM:%1$tS %1$Tp`

    1:11:31 PM

4.2.2 Entrust JASTK logging

You can enable logging for the Entrust JASTK component. On the application server, open regedit and browse to the registry key:

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJASTKConnector
```

This key contains the following values:

- `JavaLocation` – an existing value containing the path to the MyID Java components.
- `LogFile` – a String value containing the path of the JASTK log file.
- `LogLevel` – a DWORD value containing the logging level to use.

  The available logging levels, from least to most output, are:

  - `0` – off.
  - `1` – basic.
  - `2` – network, cache, and basic.
  - `3` – security, network and basic.
  - `4` – extension, security, network and basic.
  - `5` – LiveConnect, extension, security, network, temp, basic, and Deployment Rule Set.
- `CFGLogFile` – a String value containing the path to the CFG log file.
- `CFGLogLevel` – a DWORD value containing the logging level to use for the CFG log.

  The available logging levels, from least to most output, are:

  - `0` – turns off logging. This is the default value for this configuration.
  - `1-2` – errors and exceptions.
  - `3-4` – debug messages.
  - `5-7` – trace messages.
  - `8-9` – protocol I/O.

If the entries do not exist, you can create them.

For example:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJASTKConnector]
"JavaLocation"="C:\\Program Files\\Intercede\\MyID\\Components\\Java"
"LogFile"="c:\\logs\\java.log"
"LogLevel"=dword:00000005
"CFGLogFile"="c:\\logs\\java_xap.log"
"CFGLogLevel"=dword:00000004
```

To disable logging, you can set the `LogLevel` or `CFGLogFile` to `0`, or remove the `LogFile` or `CFGLogFile` entry.

Note: The difference between providing no values and a `LogLevel` or `CFGLogFile` setting of `0` is that the Java tracing will create or reset the existing log file to a file of length 0, and not produce any logging.

Note: Issuing a single certificate with a `LogLevel` of `4` produces a file over 500 KB; leaving the diagnostic running has implications for disk space.

4.2.3 Entrust JASTK Connector logging

You can also set up logging for the Entrust JASTK Connector component, which may provide some additional information.

To set up logging for the Entrust JASTK Connector component, open regedit and browse to the registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Trace\EntrustJastkConnector`

If the key does not exist, you can create it.

Create a String value with the path to the log file.

For example:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Trace\EntrustJastkConnector]
"Location"="c:\\logs\\jastk.log"
```

Note: You must ensure that the MyID named COM user has the necessary permissions to create and write to the log file. You can create a file then give the user write permissions if you prefer not to give the user create permissions.

Important: Disable the logging when you have completed diagnosing the issues, as the log file may become very large.

4.3 Auditing

The MyID audit report may contain useful information about certificate operations carried out with the Entrust server.

To run the audit report:

1. From the **Reporting** category, select **Audit Reporting**.
2. Select the search criteria; for example, from the **Operation** drop-down list, select **Certificate Requests**.
3. Click **Search**.

See the *Running the audit report* section in the ***Administration Guide*** for more information about the audit report.

Note: The order of the DN element displayed in the audit report may not match the order used for the actual certificate; internally, the DN may be stored in reverse. This does not affect the operation of the certificate.