ADSS Entrust Proxy Server Deployment – Quick Guide

This document aims to provide a quick guide to evaluate ADSS Server integration with Entrust Authority Security Manager (EASM).

Overview

The ADSS Entrust Proxy Server provides ADSS Server with the ability to issue certificates from the Entrust Certification Authority. ADSS Server sends certificate requests to the ADSS Entrust Proxy Server which then forwards the requests to an Entrust CA using the Entrust XAP subsystem. All requests are digitally signed by an Entrust Digital ID issued to the ADSS Entrust Proxy Server by an Entrust CA. ADSS Entrust Proxy Server provides the following certificate life cycle operations with the Entrust CA i.e.

- Create users and their certificates
- Renew user certificates
- Revoke or Recover user certificates.

System Requirements

To view the system requirements for ADSS Entrust Proxy Server, navigate to the link below:

ADSS Server (ascertia.com)

Required Authentication Files

ADSS Entrust Proxy Server requires the following three files to communicate with the EASM:

- **entrust.ini**
  The INI file contains the Entrust CA, XAP Service address and other entrust settings including Directory Connection setting and CA DN search base.
- **EPF file – NOTE: See Appendix A for guidance on how to create this within the Entrust CA.**
  An EPF file contains a user authentication credential and certificate to communicate with the Entrust CA.
- **sample.properties**
  The sample.properties file is used to store the Entrust CA configuration parameters. For details, refer to the Entrust Authority Security Administration Toolkit for Java Platform Programmers Guide that is bundled with the Entrust toolkit.
  - CFG_LOGIN_PROFILE – This is the Entrust Digital Identity created by the Entrust CA, this enables the ADSS Entrust Proxy to send enrollment requests to the Entrust CA.
  - CFG_LOGIN_PASSWORD – This is the password for the Entrust Digital Identity used to communicate with the Entrust CA.
  - CFG_7_URL – This is the URL required to connect to the Entrust CA XML Administration Protocol (XAP) subsystem.

The following provides an example sample.properties file:

```
CFG_LOGIN_PROFILE=C:/entrust/ADSS_XAP.epf
CFG_LOGIN_PASSWORD=caPassw0rd
CFG_7_URL=https://192.168.161.20:443
```

User can get all these files from their Entrust Administrator and place them anywhere on the local file directory where it is required to deploy ADSS Entrust Proxy Server.

Deployment in Tomcat

- Download the tomcat v10.x from location: https://tomcat.apache.org/download-10.cgi
- Extract the zipped package of tomcat in any directory (other than Windows installation directory) with full read/write permissions e.g. **D:/tomcat/**
- Set the JDK path in tomcat:
  - ***For Windows:***

    Edit the **setclasspath.bat** from location **<Tomcat Home Directory>/bin/** and add the following variable in it at top e.g.

    SET JAVA_HOME=C:\Program Files\Java\jdk11.0.19
  - ***For Linux:***

    Edit the **startup.sh** from location **<Tomcat Home Directory>/bin/** and add the following variables in it at top e.g.

    - **JAVA_HOME=/usr/java/jdk11.0.19**
    - **export JAVA_HOME**
- Extract the **adss_entrust_proxy_server.zip** to any directory from location **[ADSS Server Installation Directory]/support/**. The extracted directory contains following files:
  - docs
  - acknowledgement.txt
  - adssentrust.war
  - readme.txt
- Copy the **adssentrust.war** file from the extracted package and place it in the following location:

  <Tomcat Installation Directory>/webapps
- Start tomcat by following these instructions:
  - ***For Windows:***

    Execute the **startup.bat** file from location: **<Tomcat Installation Directory>/bin/**.
  - ***For Linux:***

    Use the following command to mark **startup.sh** file as executable before launching:

    # sh chmod +x startup.sh

    The following command will startup Tomcat:

    # sh startup.sh

A new folder will be created with the same name as that of the war file.

- Edit the **web.xml** file from location: **<Tomcat Installation Directory>/webapps/adssentrust/WEB-INF** and replace the following init parameters:
  - **ENTRUST_CONFIGURATION** value with absolute file path of **sample.properties** file e.g. **D:/sample.properties**
  - **IP_ADDRESS** value with a valid IP address of the Entrust CA e.g. 158.132.23.24
  - **PORT** value with a valid port number of the Entrust CA e.g. 829
- The ADSS Server administrator must have the latest versions of the following Entrust toolkit libraries in advance to run the ADSS Entrust Proxy:
  - Entrust Authority Security Toolkit for the Java Platform
    - enttoolkit.jar

- Entrust Authority Security Administration Toolkit for the Java Platform
  - etjastk.jar

Place the above libraries in the following location:

<Tomcat Installation Directory>/webapps/adssentrust/WEB-INF/lib/

- Restart the Tomcat server
  - Check that the proxy application is running using the following URL: http://<IP Address>:<Port>/adssentrust/proxy e.g.

    http://localhost:8080/adss/adssentrust/proxy

The default port for tomcat is 8080. Port can be changed by editing the server.xml file located at: <Tomcat Installation Directory>/conf.

ADSS Server Configuration

ADSS Server can be quickly installed for evaluation purposes. Please see the ADSS Platform Support Document for supported operating systems, databases and other related information. You can also follow this online link: https://docs.ascertia.com/adss-platform-support-report

Follow these steps to configure Entrust CA in ADSS Server:

- Launch the ADSS Server console e.g. https://localhost:8774/adss/console
- Navigate to **Trust Manager** and register the Entrust certificate chain, root and all intermediaries one by one with the purpose set to **CA (will be used to verify other certificates and CRLs -** Click here for more details).
- Navigate to **Manage CAs > Configured External CAs** and configure the Entrust CA (certificate issuing CA) here (Click here for more details).
- Navigate to **Certification Service**, create a new certification profile and configure Entrust CA as an issuing external CA in it (Click here for more details).

CN, Surname, UID and serialNumber are all supported RDN values in the Subject DN when the Entrust CA is configured, the ADSS Entrust proxy also supports multi-valued RDNs

- Navigate to **Client Manager** and Register a new client and enable the newly created certification profile to this client (Click here for more details).
- Navigate to **Server Manager** and click on the button to **Restart all Instances** to have the changes take effect.

Appendix A: How to create the XAP user for ADSS Server within the Entrust CA

The Entrust CA uses Entrust Digital Identities or Entrust Profiles to secure communications between the ADSS Entrust Proxy and Entrust XML Administration Protocol (XAP) subsystem. This appendix provides guidance on how to create a Role, Policy and Entrust Digital Identity which will enable the ADSS Entrust Proxy to be able to request certificates from an Entrust CA.

NOTE: System permissions will vary for each deployment, please consult the documentation for the Entrust Authority Security Manager for further guidance on each setting and consult your CA administrator.

Creating a user policy and role for the Ascertia Entrust Proxy profile

Each role in the Entrust CA is assigned a user policy. A new user policy and role for the Ascertia ADSS Entrust Proxy XAP profile needs to be created.

The user policy and role need to be created in the Entrust CA; the Entrust CA will issue the Ascertia ADSS Entrust Proxy XAP profile. The new user policies and roles can be created using Entrust CA Administration.

The following procedures describe how to create a new user policy and role for Ascertia XAP profiles. For more information about user policies and roles, please consult your Entrust documentation.

Create a user policy for Ascertia Entrust Proxy profile

1. Log in to Entrust CA Administration for your Entrust CA
2. In the left-hand panel, expand Security Policy > User Policies
3. Right click Administrator Policy > Copy
   - The Copy User Policy dialog box appears
4. In the Label field, enter ADSS Entrust Proxy XAP Policy
5. In the Common name field, enter ADSS Entrust Proxy XAP Policy
6. Under Policy Attributes, locate and check the tick box to enable “Permit Server Login usage”
7. Click OK
8. If you are prompted, enter password to authorise the operation, click ok

Create a role for Ascertia Entrust Proxy profile

1. Log in to Entrust CA Administration for your Entrust CA
2. In the left-hand panel, expand Security Policy > Roles
3. Right click User Administrator > Copy

   A copy of the role appears at the bottom of the list of roles in the left-hand panel, and the new role properties appear in the right panel
4. Click the Role tab in the right-hand panel
5. In the Unique name field, enter Ascertia Entrust Proxy
6. In the User Policy drop-down list, select Ascertia Entrust Proxy XAP Policy (this is the user policy that was created in the previous procedure)
7. Click the Permissions tab
8. In the Categories list, double click Groups

   The Administrative Permissions: Groups dialog box appears
9. In the Administer Groups pane:
   - To allow the role to administer all current and future groups, select All groups
   - To restrict the role to administer specific groups, select Selected groups and then add the groups the role is allowed to administer
10. Click OK to close the dialog box
11. In the Categories list, double click Searchbases

    The Administrative Permissions: Searchases dialog box appears
12. In the Administer Searchbases pane:
    - To allow the role to access all current and future searchbases, select All searchbases
    - To restrict the role to administer specific searchbases, select Selected searchbases and then add the searchbases to the searchbases the user is allowed to administer
13. Click OK to close the dialog box
14. In the Categories list, double click Security Policy

    The Administrative Permissions: Security Policy dialog box appears
15. Select Force CRLs
16. Click OK to close the dialog box
17. In the Categories list, double click User Templates

    The Administrative Permissions: User Templates dialog box appears
18. In the Administer Templates pane:
    - To allow the role to access all current and future user templates, select All templates
    - To restrict the role to administer specific user templates, select Selected templates and then add the templates to the Selected Templates the user is allowed to administer
19. Click OK to close the dialog box
20. In the Categories list, double click Users

    The Administrative Permissions: Users dialog box appears

21. Under the User - Advanced tab, select the following permissions:
    - Change user's role
    - Modify group membership
    - Perform PKIX requests
22. Click OK to close the dialog box
23. Click Apply
24. If you are prompted, enter password to authorise the operation, click ok

Creating a user entry for the Ascertia Entrust Proxy profile

An entry in the Entrust CA needs to be created for the Ascertia Entrust Proxy profile. The Entrust CA Administration can be used to create a user entry for the Ascertia Entrust Proxy profile

This section contains the following procedures:

1. Log in to Entrust CA Administration for the Entrust CA
2. In the left-hand panel right click Users > New User
3. The New User dialog box appears.
4. Click the Naming tab, and then complete the following:
    a. Type – Person
    b. First Name – ADSS Entrust
    c. Last Name – Proxy
    d. Add to drop-down list, select the searchbase where the user entry needs to be added
5. Select the General tab
6. In the User role drop-down list, select Ascertia Entrust Proxy (this is the role that was created earlier)
7. Select the Certificate Info tab
8. In the Category drop-down list, select Enterprise
9. Under Certificate Type, select Admin Services User Registration
10. Click OK
11. enter password to authorise the operation If a prompt appears and click ok
12. Click Ok to dismiss the dialog displaying authorisation codes and reference numbers

Creating the Ascertia Entrust Proxy profile

The Ascertia Entrust Proxy profile must be an Entrust profile (EPF file) stored on software; the Ascertia Entrust Proxy does not support Entrust profiles stored on a hardware device.

1. Log in to Entrust CA Administration for your Entrust CA
2. In the right-hand panel, right-click the ADSS Entrust Proxy entry you just created and then select Create Profile
3. The Create profile dialogue box appears
4. Click Create a Desktop profile
5. In the Name field, enter the file name for the Ascertia Entrust Proxy profile (Security Manager Administration will append the .epf extension to the file name)
6. Click Browse to select a folder where the Ascertia XAP profile needs to be stored
7. In the Password and Confirm fields, enter a password for the Ascertia XAP profile
8. Click OK

Appendix B: Example Configuration

In order to issue certificates from the Entrust CA the following outlines the high-level steps that need to be performed to the Entrust CA and ADSS Server, please consult the core product documentation for further details as the following is provided as an example.

The following will add a user to the Entrust CA that enables you to issue certificates with a standard relative distinguished name like the following:

```
CN=John Doe, OU=Users, O=Ascertia Ltd, C=GB
```

The following changes will also enable you to issue certificates with multi-valued relative distinguished names like the following:

```
CN=John Doe+serialNumber=12345, OU=Users, O=Ascertia Ltd, C=GB
```

or

```
CN=John Doe+serialNumber=12345+uid=54321, OU=Users, O=Ascertia Ltd, C=GB
```

Please note that if you require the Entrust CA to publish certificates with multi-valued RDN's to the Security Manager directory then your LDAP directory server must support multi valued RDN's, if you require UID in the RDN and LDAP publication then further LDAP configuration may be required, please consult the documentation for your LDAP server on how to achieve this.

EASM Configuration

Configuring the Entrust usertype template

1. Log in to Entrust CA Administration for your Entrust CA
2. Select File > User Templates > Export, save the usertype.template to the desktop
3. Open the usertype.template in notepad and locate the following section:

```
[User Type Template List]
count=3
0=Person
1=Web Server
2=Organizational Unit
```

4. Make the following highlighted changes:

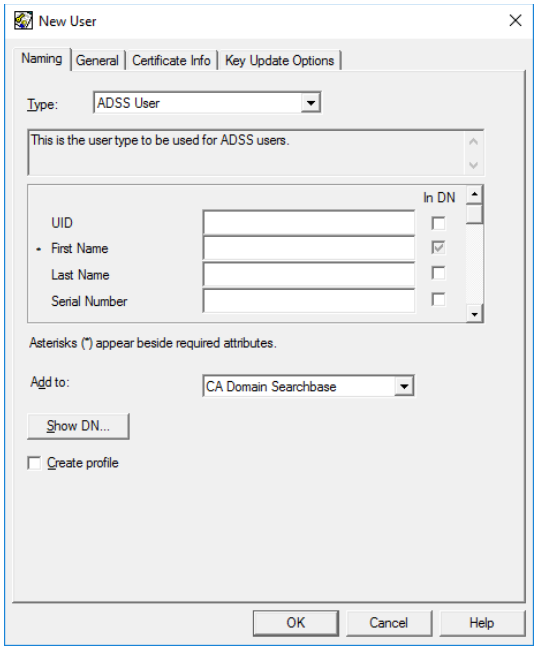
```
[User Type Template List]
count=4
0=Person
1=Web Server
2=Organizational Unit
3=ADSS User
```

5. Locate [Organizational Unit] and after this section add the following, save the changes and close notepad:

```
[ADSS User]
id=3
count=5
Structural Object Class=inetorgPerson,organizationalPerson,person descri
ption=This is the user type to be used for ADSS users.
0=UID,uid,0,0,0
1=First Name,cn,1,0,0
2=Last Name,sn,0,0,0
```

```
3=Serial Number,serialNumber,0,0,0,uniquelyIdentifiedUser
4=Email,mail,2,0,0,rfc822MailUser
```

6. Return to Security Manager Administration for the Entrust CA
7. Select File > User Templates > Import, browse to the usertype.template to the desktop and import the usertype.template you edited, save the log to the desktop
8. In Security Manager Administration right click Users and select New User, the new User dialog will have the following in the New User dialog if you select ADSS User from the type dropdown:



9. Click Cancel to close the new user dialog

Optional: Entrust master.certspec configuration

Please note, this step is **optional** and the following is only required if you do not wish to publish certificates to the Entrust CA Directory. In this sample configuration we will be issuing the nonrepudiation certificate from the Entrust ent_nonrepud certificate type.

1. Log in to Security Manager Administration for the Entrust CA
2. Select File > Certificate Specifications > Export, save the master.certspec to the desktop
3. Open the master.certspec in notepad and locate the [Advanced Settings] section
4. Add the following for the certificate type you wish to issue and not publish to the Security Manager directory:

```
[ent_nonrepud Advanced]
noUserInDirectory=1
```

5. Save and close the master.certspec
6. Select File > Certificate Specifications > Import, browse to the master.certspec to the desktop and import the master.certspec you edited, save the log to the desktop

ADSS Server Configuration

Trust Manager Configuration

1. Log into ADSS Server and the Trust Manager Tab, click the New button
2. The Trust Manager > New page will display, browse to the Entrust CA Certificate and enter a friendly name in the TA Friendly Name field, check the CA tick box, and click Finish.

Managed CA Configuration

1. Select the Manage CAs tab
2. Select External CAs, click the new button
3. Enter the following information in the New External CA Settings page:

   CA Alias: Entrust - NonRepudiation
   CA Type: Entrust CA
   Entrust Proxy: http://localhost:8080/adssentrust/proxy
   Certificate Type: ent_nonrepud
   Certificate Purpose: Nonrepudiation
   User Type: ADSS User
   Publish Certificate At: Database (NO_OP)
   CA Distinguished Name: OU=Users, O=Ascertia Ltd, C=GB

   NOTE: When using the Publish Certificate At: Database (NO_OP) setting, at the Entrust CA the following must be set in the master.certspec, for further information consult the Entrust documentation:

```
[ent_nonrepud Advanced]
noUserInDirectory=1
```

4. Click test to test the connection to the Entrust CA, click close once the teat has completed, click Save.
5. At the External CAs page click the Service Manager link and click Restart All Instances

Certification Service Configuration

1. Select the Certification Service tab
2. Select Certification Profiles, click the new button
3. Enter the following in the New Certification Profiles page and click Save:

   Profile Name: Entrust_NonRepudiation
   Automatically process requests: Checked
   Enable key pair generation through RAS Service: Unchecked
   CA Details: Use External online CA – External CA: Entrust CA - NonRepudiation
   Crypto Profile: Software
   Key Algorithm: RSA – Overridable: Checked
   Key Length: 2048 – Overridable: Checked
   Subject Distinguished Name: CN=$CN,UID=$UID,SERIALNUMBER=$SERIALNUMBER– Overridable: Checked
   Match the pattern with subject DN in request: Unchecked – Overridable: Checked
   Validity Period: 12 Months
   Valid From: Time of Issuance
   Certificate Renewal Settings: Renew Certificate

4. At the Certification Profiles page click the Client Manager link to assign the new profile to a client

Client Manager Configuration

1. The Client Manager page will display, click New
2. The New page will display, on the General Tab enter the following click save:

```
Client ID: Entrust
Friendly Name: Entrust
```

3. You will be returned to the Client Manager page, click on the Entrust client ID
4. Under the Entrust client select the Certification Service tab
5. Check the “Allow this client to access the ADSS Certification Service” check box
6. Select the Entrust_NonRepudiation certification profile and add this to the Selected Certification Profiles list, click Save.

7. Select the Service Manager link that appears and restart the Certification Service

The following are examples of tests that can be run using the ADSS Server Test Tool.

User with simple RDN

Entrust - `cn=Michael Caine, ou=Users, o=Ascertia Ltd, c=GB`

OpenSSL - `C=GB, O=Ascertia Ltd, OU=Users, CN=Michael Caine`

Microsoft certutil -

```
Subject:
    CN=Michael Caine
    OU=Users
    O=Ascertia Ltd
    C=GB
```

```
-service certification -server http://localhost:8777/adss/certification/csi -
mode xml -out data/certification/output -action create -client entrust -
profile adss:certification:profile:005 -subject "CN=Michael Caine" -password
password -alias MichaelCaine -verbose
```

User with multi-valued RDN CN and serialNumber

Entrust - `cn=Kate Winslet + serialNumber=kw-12345, ou=Users, o=Ascertia Ltd, c=GB`

OpenSSL - `C=GB, O=Ascertia Ltd, OU=Users/serialNumber=kw-12345, CN=Kate Winslet`

Microsoft certutil –

```
Subject:
    SERIALNUMBER=kw-12345 + CN=Kate Winslet
    OU=Users
    O=Ascertia Ltd
    C=GB
```

```
-service certification -server http://localhost:8777/adss/certification/csi -
mode xml -out data/certification/output -action create -client entrust -
profile adss:certification:profile:005 -subject "CN=Kate
Winslet,SERIALNUMBER=kw-12345" -password password -alias KateWinslet -verbose
```

User with multi-valued RDN CN, serialNumber and UID

Entrust - `uid=MB12345 + cn=Marlon Brando + serialNumber=MB-12345, ou=Users, o=Ascertia Ltd, c=GB`

OpenSSL - `C=GB, O=Ascertia Ltd, OU=Users/serialNumber=MB-12345, CN=Marlon Brando/UID=MB12345`

Microsoft certutil -

```
Subject:
    SERIALNUMBER=MB-12345 + CN=Marlon Brando + uid=MB12345
    OU=Users
    O=Ascertia Ltd
    C=GB
```

```
-service certification -server http://localhost:8777/adss/certification/csi -
mode xml -out data/certification/output -action create -client entrust -
profile adss:certification:profile:005 -subject "CN=Marlon
Brando,SERIALNUMBER=MB-12345,UID=MB12345" -password password -alias
MarlonBrando -verbose
```

Appendix C: Managing Multi-Valued RDNs in Certificate Issuance via Entrust Proxy

When issuing a certificate to a user with a multi-valued Relative Distinguished Name (RDN), the Entrust Proxy Server may encounter issues. Specifically, it sends only a partial Common Name (CN) to the Entrust CA, leading to failures in certificate creation. For example, if the CN is defined as CN=Brian Williams, the Entrust Proxy Server transmits only CN=Brian because it interprets Williams as the surname (SN), which may be disabled or not required the Entrust Template using the overrideCommonNameForma-t=0 setting.

Behavior of ADSS Entrust Proxy

To address this issue, the ADSS Entrust Proxy retrieves the `overrideCommonNameFormat` property from the user template in Entrust CA. This property is used to format the CN and parse the Last Name (SN) based on specific settings.

Common Name (CN) Formatting

The Entrust Proxy fetches the `overrideCommonNameFormat` property from the user type settings in Entrust. Based on this value, Subject Distinguished Names (SDNs) are formatted as follows:

1. If **`overrideCommonNameFormat = Disabled:`**

   The CN in the request remains unchanged in the certificate.

   a. Example 1:

      i. Request: CN=Brian John Williams

      ii. Certificate: CN=Brian John Williams

   b. Example 2:

      i. Request: CN=www.ascertia.com

      ii. Certificate: CN=www.ascertia.com

2. If **`overrideCommonNameFormat = 1:`**

   The CN is parsed, and all elements except the last are used as the first name, while the last element is used as the surname.

   a. Example:

      i. Request: CN=Brian John Williams

      ii. Certificate: Firstname=Brian John, Surname=Williams
      (CN=Brian John Williams)

3. If **`overrideCommonNameFormat = 2:`**

   The Entrust CA reverses the CN contents to display the surname first, followed by the first name. The processing logic remains consistent, parsing the CN as above.

   a. Example:

      i. Request: CN=Brian John Williams

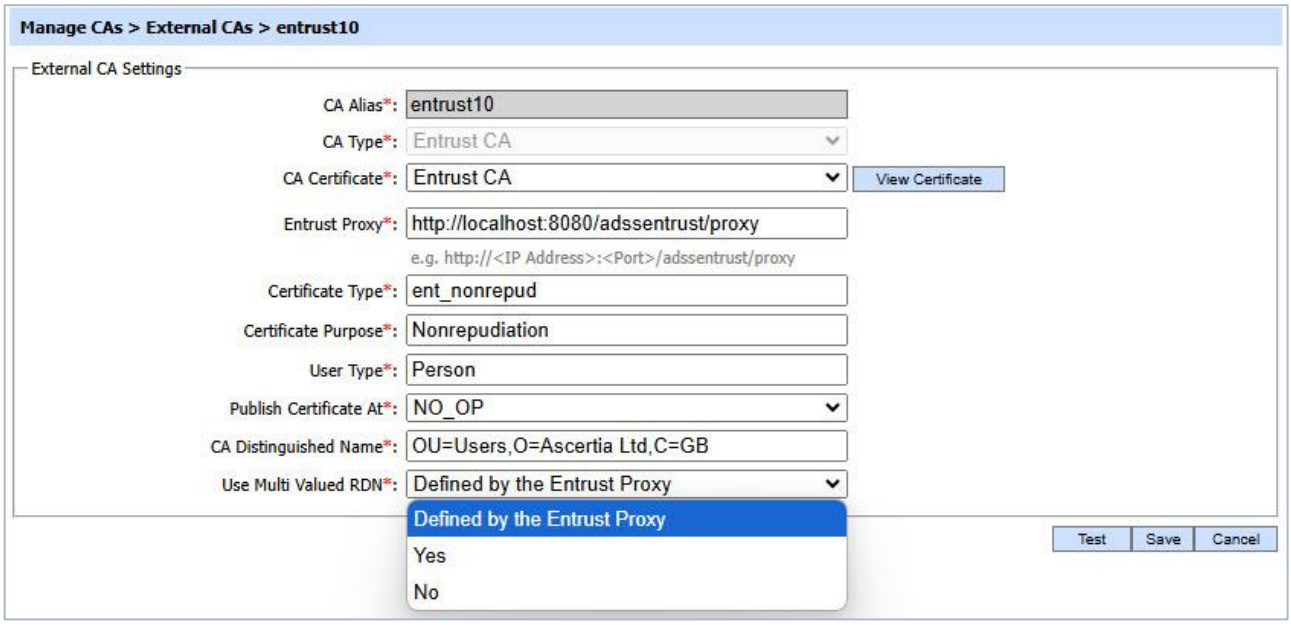
      ii. Certificate: Surname=Williams, Firstname=Brian John
      (CN=Williams, Brian John)

LDAP Considerations

If LDAP publication of user certificates is required, an LDAP object class should be used that does not mandate a surname. This is necessary because the surname will not be included in the user creation request sent to the Entrust CA.

ADSS Server External CA configurations for Multi-valued RDN

A 'Use Multi Valued RDN' drop-down field is available on External CA > Entrust CA screen:



The Use Multi-Valued RDN field is a drop-down option that allows administrators to control how the Common Name (CN) is managed during the certificate creation process. It offers three selectable options.

- **Defined by the Entrust Proxy:** When this option is selected, the `CREATE_USER_WITH_FULL_PARAMS` property value will be used as per proxy settings defined in the web.xml file located at [Apache-Tomcat-Installation-Directory]\webapps\adssentrust\WEB-INF\web.xml.
- **Yes:** If this option is selected, the ADSS Server will send TRUE in the certificate creation request. This prompts the ADSS Entrust Proxy to override the settings specified in the web.xml file and prioritize the values send by the ADSS Server. Here, the Entrust will create the user with full subject RDN including (CN+UID+Serial Number).
- **No:** If this option is selected, the ADSS Server will mandate the ADSS Entrust Proxy to create the user using only the CN (Common Name) in the Subject DN, without including any additional information.

Please keep the below points under consideration:

1. *The Entrust Proxy will prioritize the value selected on ADSS Console.*
2. *The `CREATE_USER_WITH_FULL_PARAMS` parameter value can be included in the HTTP request header. If it is provided in the HTTP header, the value specified here will have a lower priority.*

Appendix D: How to publish certificates at Database or LDAP

The Entrust CA can publish the requested certificates to both local databases or LDAP directory. This appendix provides guidance steps on how to publish the certificates at both databases and LDAP.

Publish certificates to only the Entrust CA Databases:

Follow the below steps in order to publish the certificates at databases:

1. Export master.certspec file to the file system
2. Edit the master.certspec file and uncomment these two lines (if commented)
   a. `[ent_nonrepud Advanced]`
   b. `noUserInDirectory=1`
3. Save the file
4. Import the master.certspec file and then generate the certificate

Generate certificate with full parameters:

Below is the supported **RDN's** list for databases:

- **CN** - Common Name
- **G** - Given Name
- **SN** - Surname
- **OU** - Organization Unit
- **O** - Organization
- **E** - Email
- **L** - Locality
- **ST** - Street Address
- **S** - State
- **P** - Postal Code
- **C** – Country
- **SERIALNUMBER** - Subject Serial Number
- **UID** - Unique Identifier

In order to generate a Certificate with full parameters where **'CN', 'SERIALNUMBER'** and **'UID'** are merged in a single Common Name RDN of a certificate, follow the instructions below:

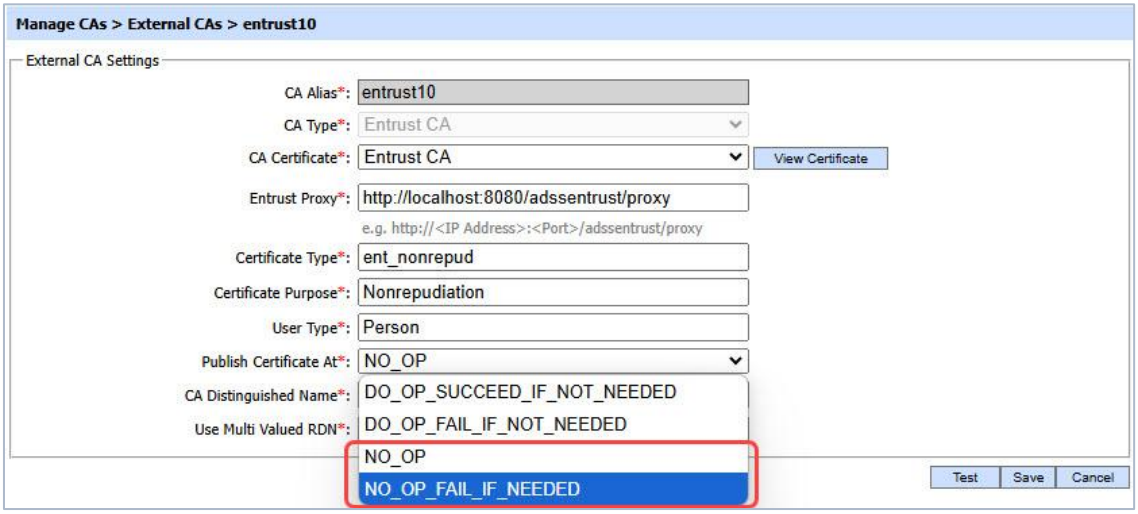
1. Go to `<Tomcat>/webapps/adssentrust/WEB-INF/web.xml`
2. Edit web.xml file
3. Find this parameter if exists then mark the parameter value TRUE otherwise add this parameter and save the file:

```
<init-param>
        <param-name>CREATE_USER_WITH_FULL_PARAMS</param-name>
        <param-value> TRUE </param-value>
 </init-param>
```

4. Restart Tomcat

Within the ADSS Server Console, select the below options for creating user certificates in the CA Database only under Manage CAs → External CAs → Entrust CA:

DO_OP_SUCCEED_IF_NOT_NEEDED	Perform the LDAP operation
DO_OP_FAIL_IF_NOT_NEEDED	Perform the LDAP operation (fail if not needed)
NO_OP	Skip the LDAP operation
NO_OP_FAIL_IF_NEEDED	Skip the LDAP operation (fail if needed)



Publish certificates to the Entrust CA LDAP:

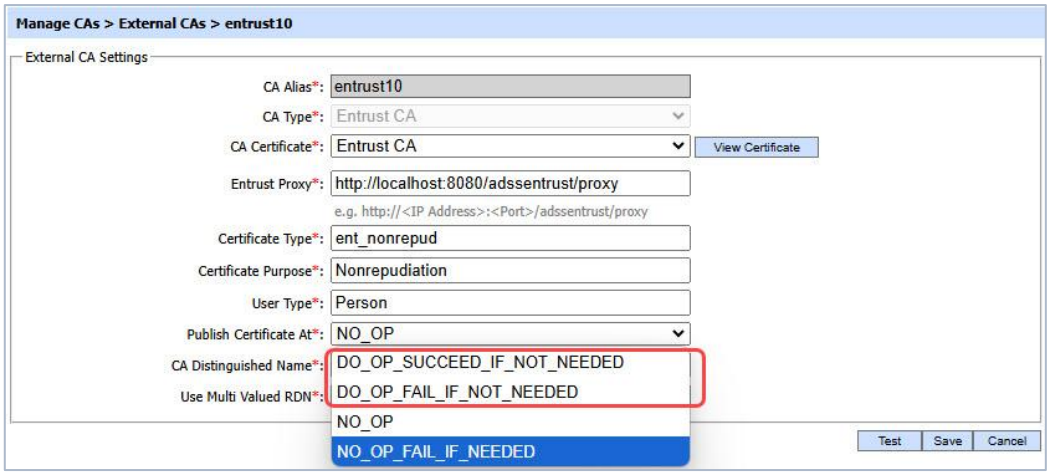
Follow the below steps in order to publish the certificates to the Entrust CA LDAP:

1. Export master.certspec file to the file system
2. Edit the master.certspec file and comment these two lines
   a. `[ent_nonrepud Advanced]`
   b. `noUserInDirectory=1`
3. Save the file
4. Import the master.certspec file and then generate the certificate
5. You can view the certificates published to the Entrust CA LDAP using the directory browser in Entrust CA Administration.

Note: If you require the Entrust CA to publish certificates with multi-valued RDN's to the Security Manager directory then your LDAP directory server must support multi valued RDN's, if you require UID in the RDN and LDAP publication then further LDAP configuration may be required, please consult the documentation for your LDAP server on how to achieve this.

Within the ADSS Server Console, select the below options for creating user certificates in the CA Database and publishing to the Entrust CA LDAP under Manage CAs → External CAs → Entrust CA:

DO_OP_SUCCEED_IF_NOT_NEEDED	Perform the LDAP operation
DO_OP_FAIL_IF_NOT_NEEDED	Perform the LDAP operation (fail if not needed)
NO_OP	Skip the LDAP operation
NO_OP_FAIL_IF_NEEDED	Skip the LDAP operation (fail if needed)



Contact Details

For Commercial Sales: +44 (0) 1256 895416, sales@ascertia.com

For Technical Support: support@ascertia.com

*** End of Document ***