

Entrust Certificate Authority Comprehensive (ECAC) Lab Book

This companion lab book provides step by step exercises for lessons of the Entrust Certificate Authority Comprehensive Course (PKI) for v10 and must be completed in a lab environment provided by the instructor.



ECAC Lab book V3 Nov2020



Copyright©2020 Entrust. All rights reserved

Entrust is a trademark of Entrust Inc. in certain countries. All entrust product names and logos are trademarks or registered trademarks of Entrust, Inc in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

The information contained in this document may not be duplicated in part or in whole without prior written approval of Entrust.

Security Concepts

This module introduces the processes and technologies of PKI security. There is no hands on lab for this module but there are discussion questions as a review.

Discussion Questions

- 1 How does the encryption operation provide privacy to the data?
- 2 How is it ensured that only the intended recipient has access to the data?
- 3 How does the digital signature process provide data integrity and non-repudiation?
- 4 If the key used to decrypt data is also used to sign data, what issues of non-repudiation are brought into question?
- 5 What could be a possible solution to these issues?
- 6 In the digital signature process, the sender's public verification key is attached to the signed message package. What benefit could this provide over storing the verification key in the public repository?
- 7 Which of the basic security requirements are fulfilled by the encryption process? Which are fulfilled by the digital signature process?

Digital Certificates

This module introduces the format and content of a Digital Certificate. There is no hands on lab for this module but discussion questions as a review.

Discussion Questions

- 1 Are Certificates encrypted? Why or Why not?
- 2 Why is it important that many policy decisions be determined before deploying Entrust Authority Security Manager?
- 3 Below describe how a Certificate is created by the CA.

Entrust Certificate Authority

This module introduces the Entrust Certificate Authority. There is no hands on lab for this module but discussion questions as a review.

Discussion Questions

- 1 If CA key compromised and cert revoked, how is user affected?
- 2 If the CA acts as a trust anchor, why do we trust the CA?
- 3 What are the purpose of Link Certificates?

Entrust PKI

This module introduces the Entrust PKI. There is no hands on lab for this module but discussion questions as a review.

Discussion Questions

- 1 Why do separate roles exist in SM?
- 2 Why is the Directory on a separate server?
- 3 What is the benefit of High Availability for the Database?

Role of the Directory and Database

This module introduces the Directory and Database as repositories. There is no hands on lab for this module but there are discussion questions. After the PKI is installed we will revisit these concepts.

Discussion Questions

- 1 What is the effect of changing the DIT after the CA is in use?
- 2 The Directory experiences a DOS attack
 - a. How will this affect users?
 - b. How will this affect administrators
 - c. How will this affect SM?
- 3 List considerations for High Availability for the PKI Database.
- 4 Describe the purpose of the bootstrap information

Installing Entrust Authority Security Manager

In this module you will install the Entrust Authority Security Manager 10 product and perform an initialization. This will set the initial parameters for the CA and identify the Master Users and First Officer. You will also set credentials for user accounts necessary for CA communications.

Lab

In these exercises, participants will install, configure and initialize Entrust Authority Security Manager 10 on a Windows Server 2019.

Record all installation options on the *Installation and configuration planning worksheets contained in Appendix A of this Lab Manual*.

Tasks

The following tasks will be completed:

Exercise 1: Install the Entrust Authority Security Manager database

Exercise 2: Install Entrust Authority Security Manager

Exercise 3: Configure Security Manager

Exercise 4: Initialize Entrust Authority Security Manager

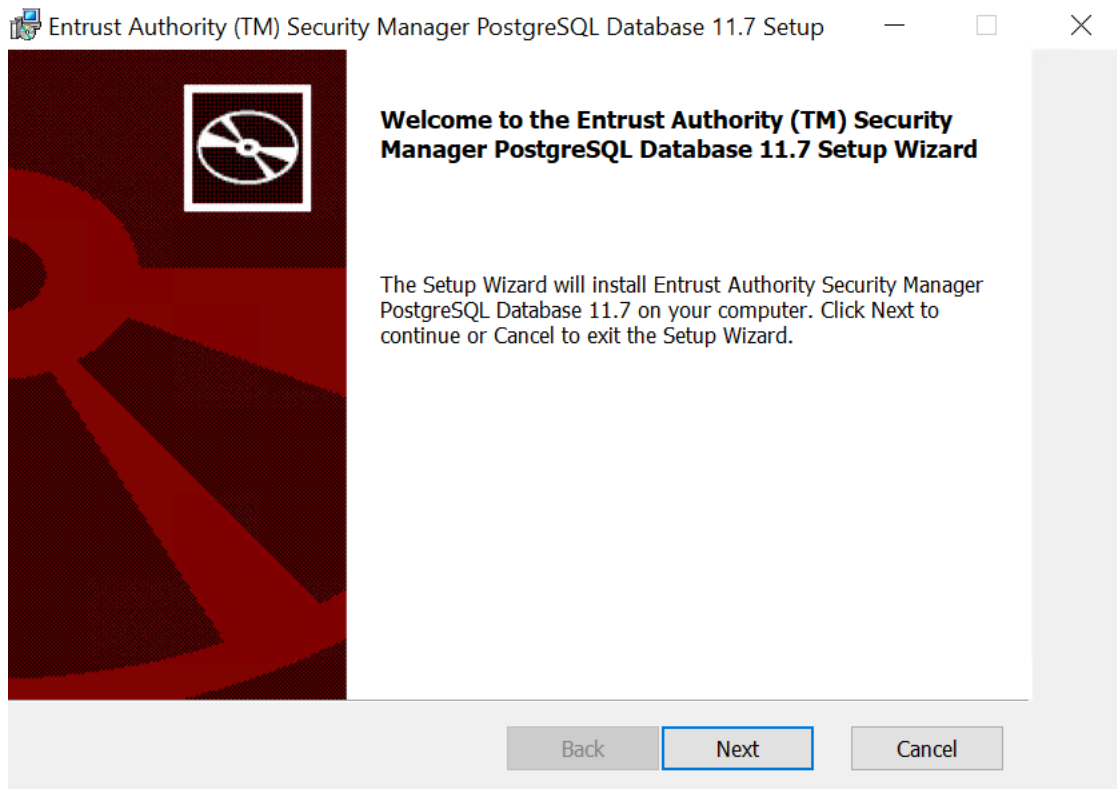
Timing

Estimated time to complete these exercises is 45 minutes

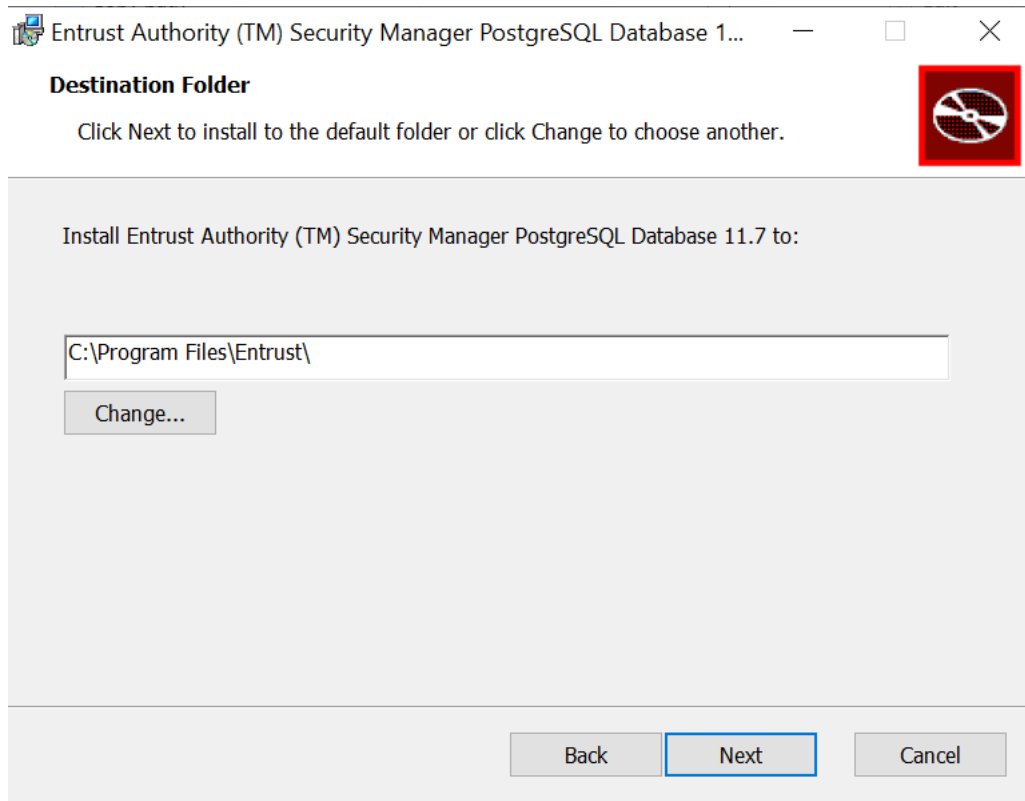
Exercise 1: Install the Entrust Authority Security Manager database

The database must be in place before the installation of the Entrust Authority Security Manager can be attempted. In this exercise, a PostgreSQL database provided by Entrust will be installed to store all Entrust Authority Security Manager related information.

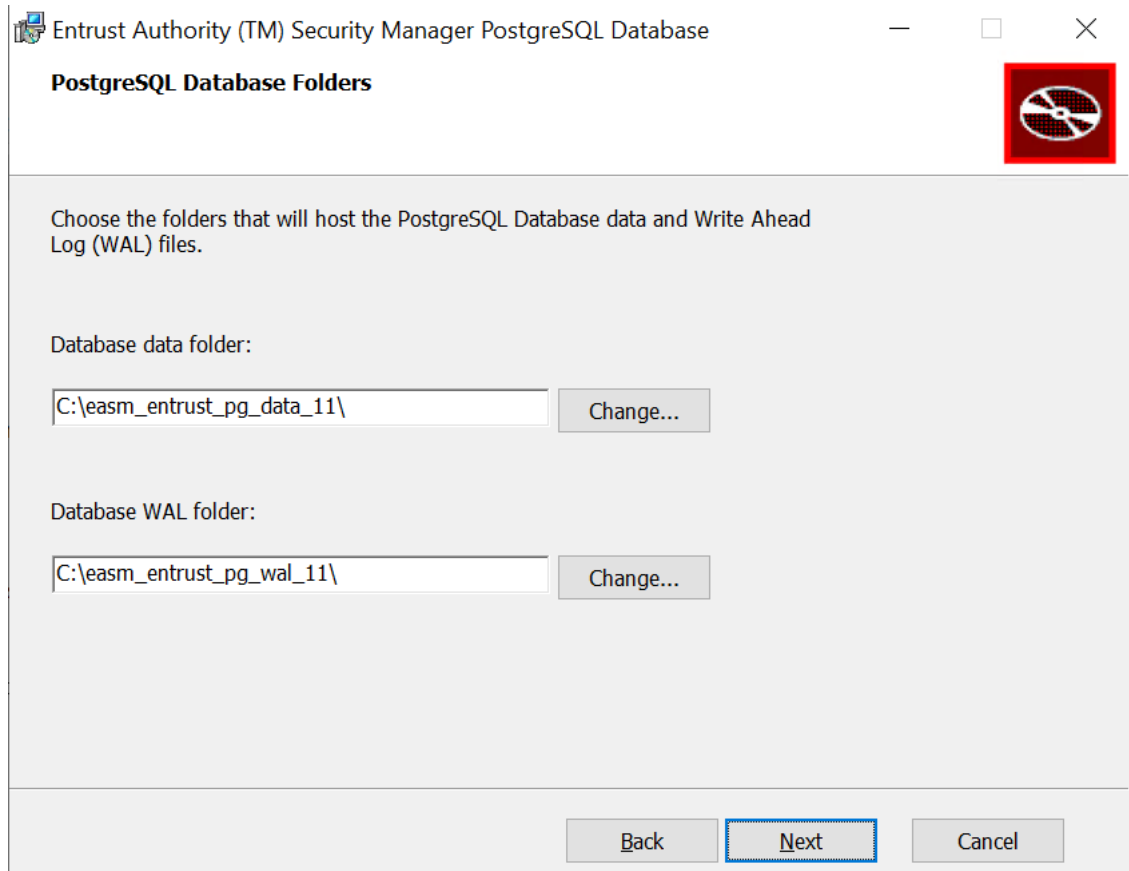
- 1 Locate the `SecurityManager_PostgreSQL` file in the `C:/Source/SM 10.0` folder. Double-click the file to start the installation program.
- 2 The Entrust Authority Security Manager PostgreSQL installation wizard is presented. Click **Next** to begin the wizard.



- 3 Identify the location to install the Database. Leave the default and click Next.

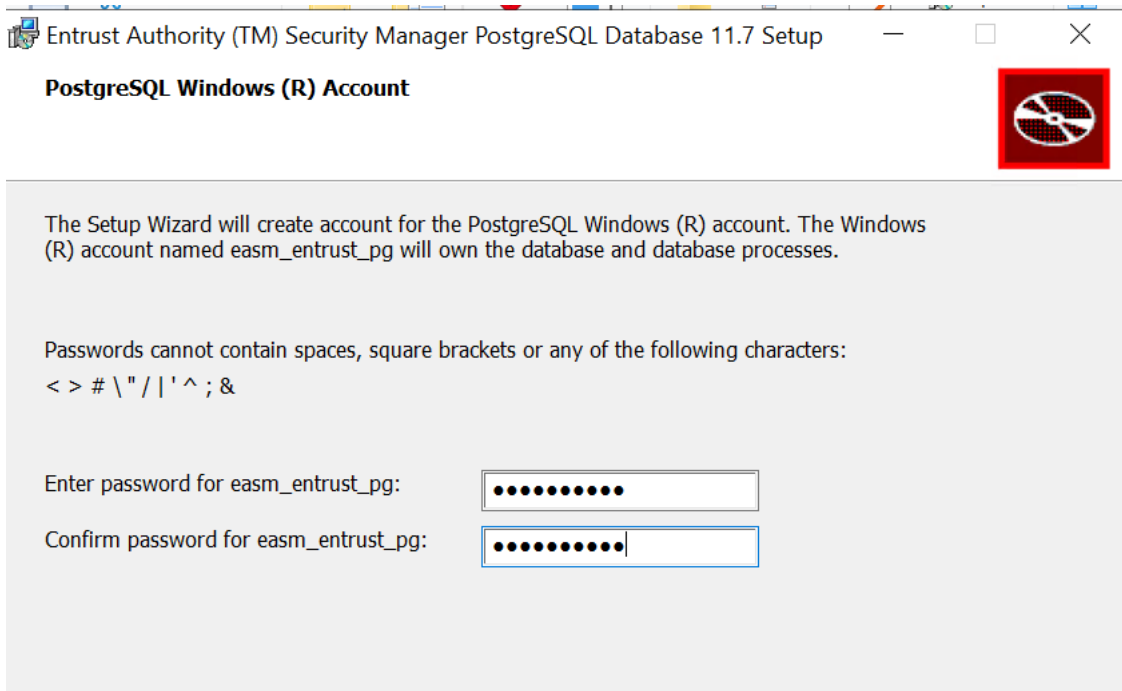


- 4 Also accept the default locations for the data and WAL folders.



- 5 Type and confirm a password for the PostgreSQL Windows user account called `easm_entrust_pg` that is created by the installation.

This account owns the PostgreSQL database and database processes. In the classroom, type a password of `EntPKI2000` and click **Next**.

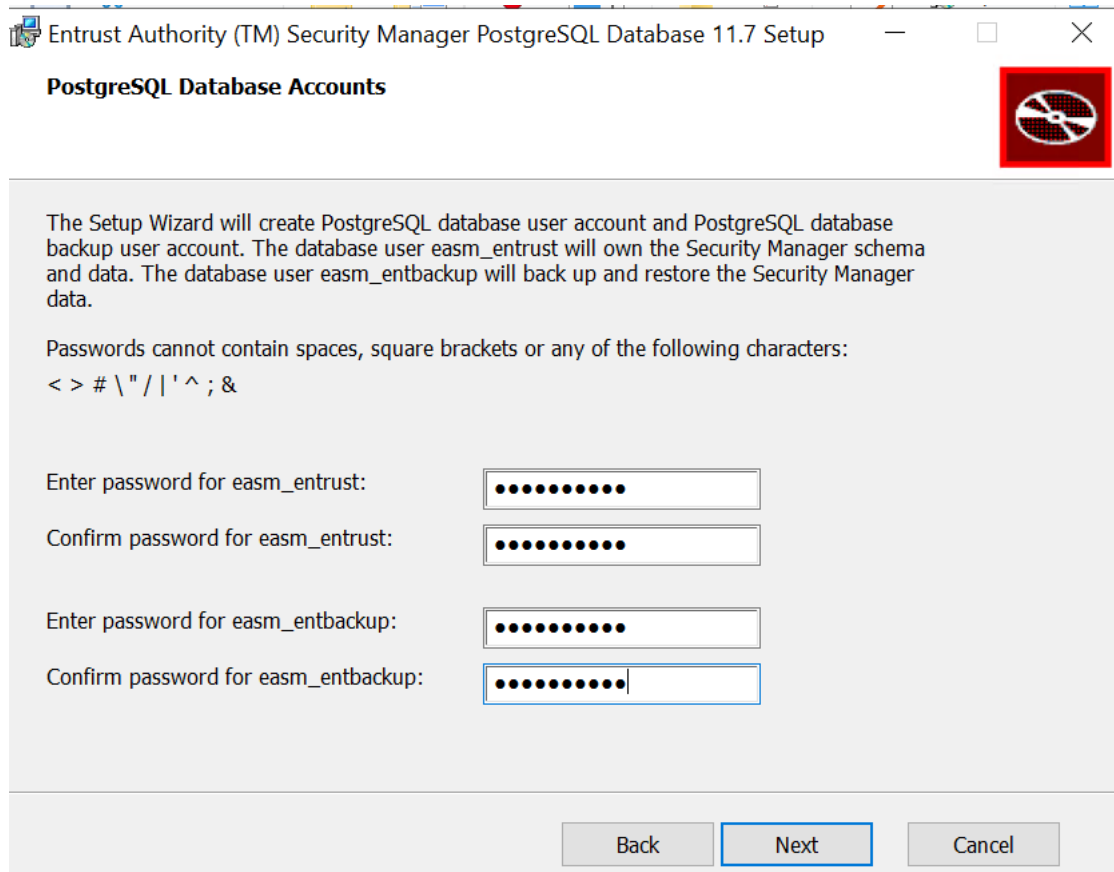


Note:

Use the suggested password in the classroom environment as it will allow the instructor to access your infrastructure if any modifications must be made during the course.

- 6 Type and confirm a password for the PostgreSQL account called `easm_entrust_pg`. This user account will own the Entrust Authority Security Manager schema and data in the database. Type the password of `EntPKI2000`.

- 7 Type and confirm a password for the PostgreSQL database user account called `easm_entrust`, and the backup user account `easm_entbackup`. This database user is required to back up and restore Entrust Authority Security Manager data. Type the password of `EntPKI2000` and click **Next**.



PostgreSQL Database Accounts

The Setup Wizard will create PostgreSQL database user account and PostgreSQL database backup user account. The database user `easm_entrust` will own the Security Manager schema and data. The database user `easm_entbackup` will back up and restore the Security Manager data.

Passwords cannot contain spaces, square brackets or any of the following characters:
< > # \ " / | ' ^ ; &

Enter password for `easm_entrust`:

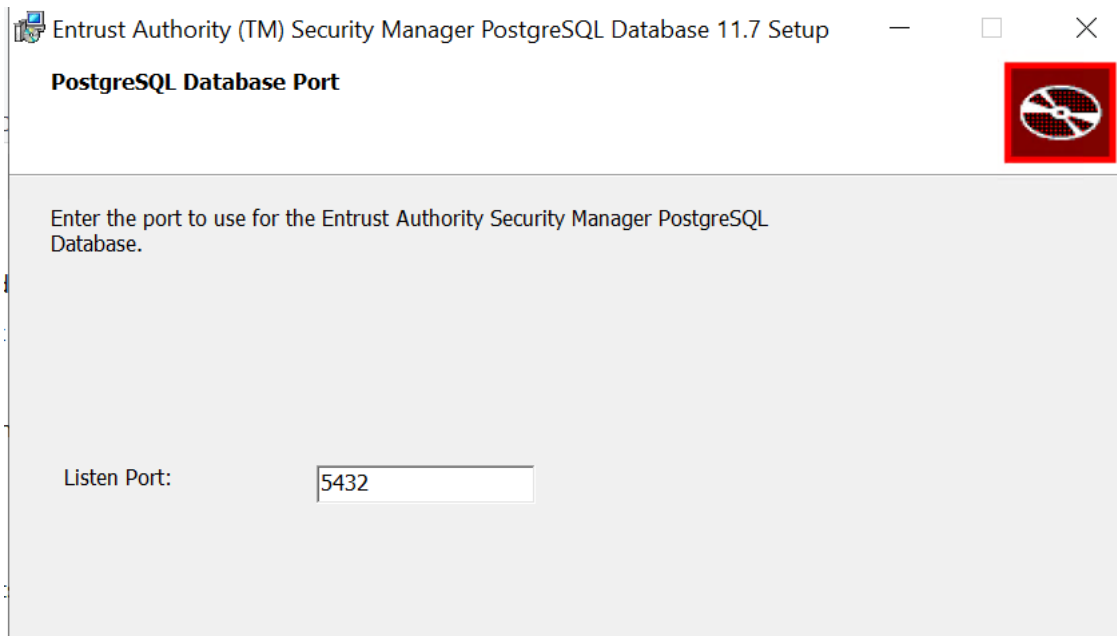
Confirm password for `easm_entrust`:

Enter password for `easm_entbackup`:

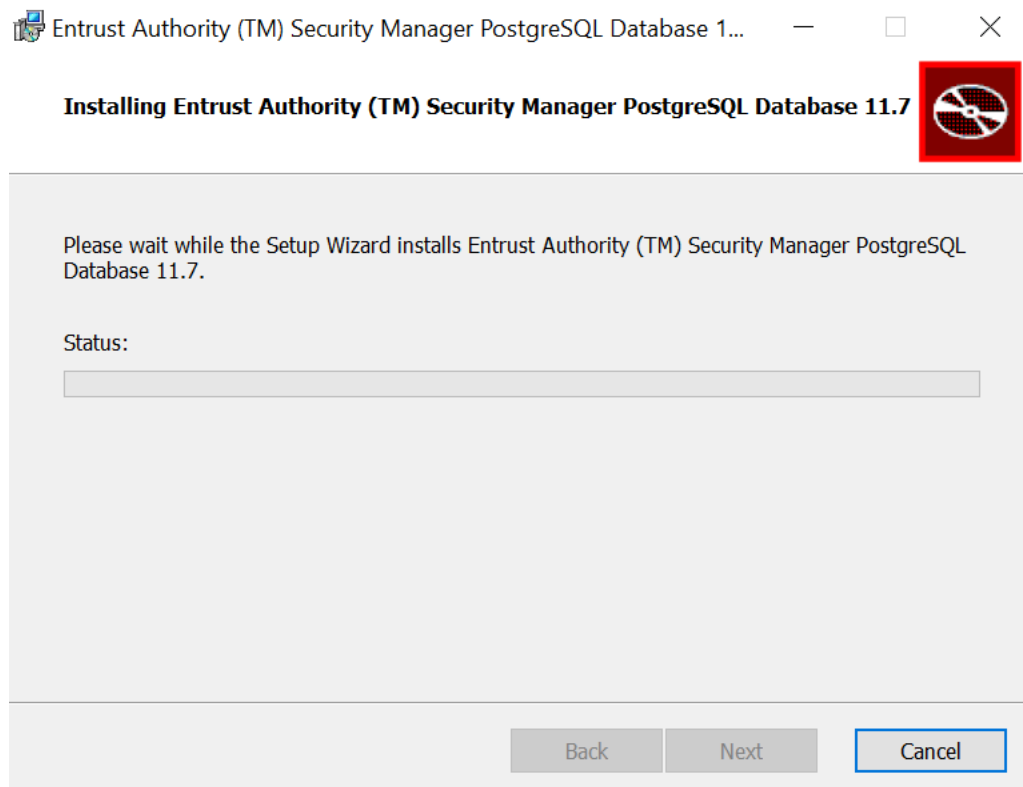
Confirm password for `easm_entbackup`:

Back Next Cancel

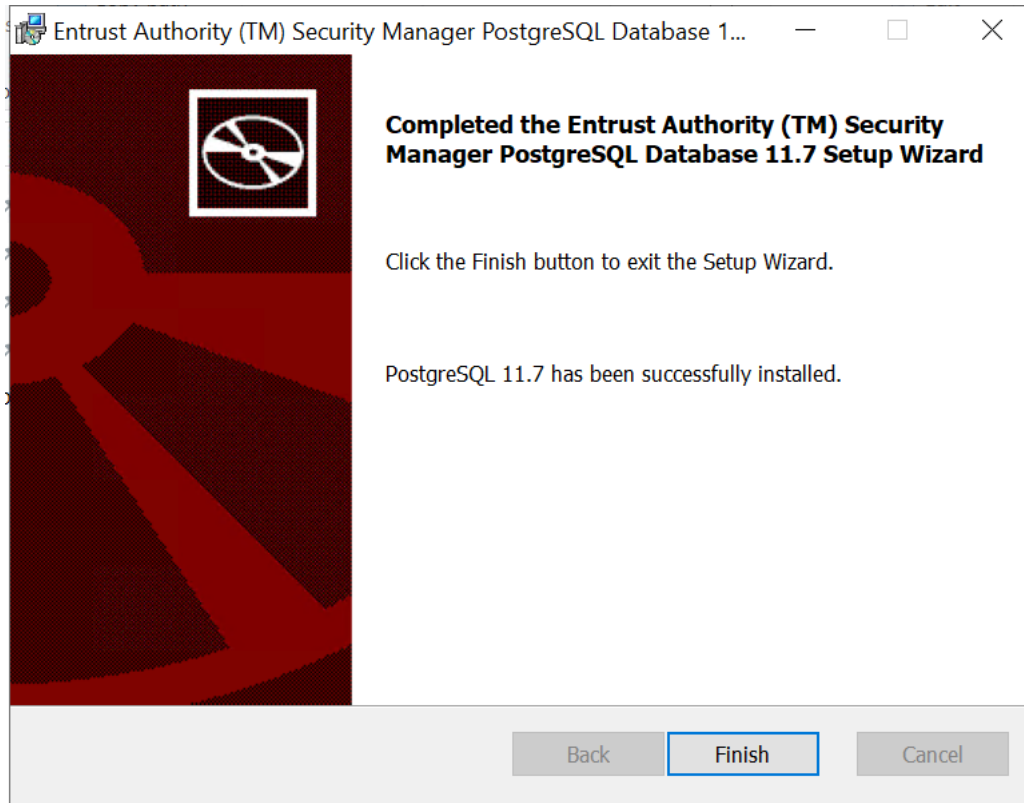
- 8 Accept the default communication port used by PostgreSQL of 5432 and click **Next**.



- 9 Click **Install** to install PostgreSQL.
A status bar displays the progress of the installation.



10 Click **Finish** to complete the installation.



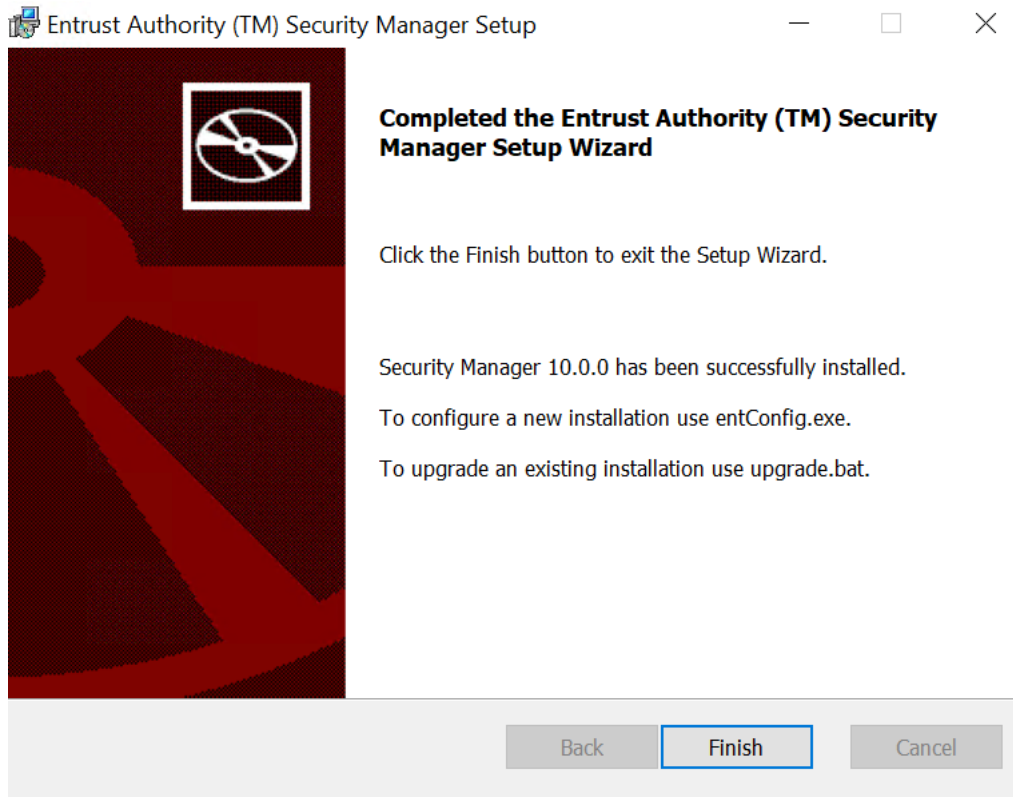
Note:

If any errors are encountered during installation, open the `postgres3.log` file in the `C:\leasm_entrust_pg_data_11\log` folder for more details.

Exercise 2: Install Entrust Authority Security Manager

In this exercise, the Entrust Authority Security Manager program files will be installed.

- 1 Locate the `SecurityManager.10.0.0.609` installer file from the `Source/SM 10.0` folder. Double-click the file to start the installation program.
- 2 The files will be extracted from the archive. This process may take a few minutes.



- 3 The Entrust Authority Security Manager installation wizard will complete and you can click Finish.

Exercise 3: Configure Security Manager

- 1 Browse to the **C:\Program Files\Entrust\Security Manager\bin** folder and launch **entConfig**
- 2 A popup window will identify we have a Database installed and will ask if you want to use it. Select Yes.

Database Deployment Model



The Security Manager Configuration has found an installation of the Entrust Authority (TM) PostgreSQL database on this host. The installation location is at: 'C:\Program Files\Entrust\easm_postgres11\'.
Do you want to use it as an embedded database deployment for Security Manager?

Yes

No

- 3 The Configuration welcome screen appears. Select Next.



Entrust Authority(TM) Security Manager Configuration



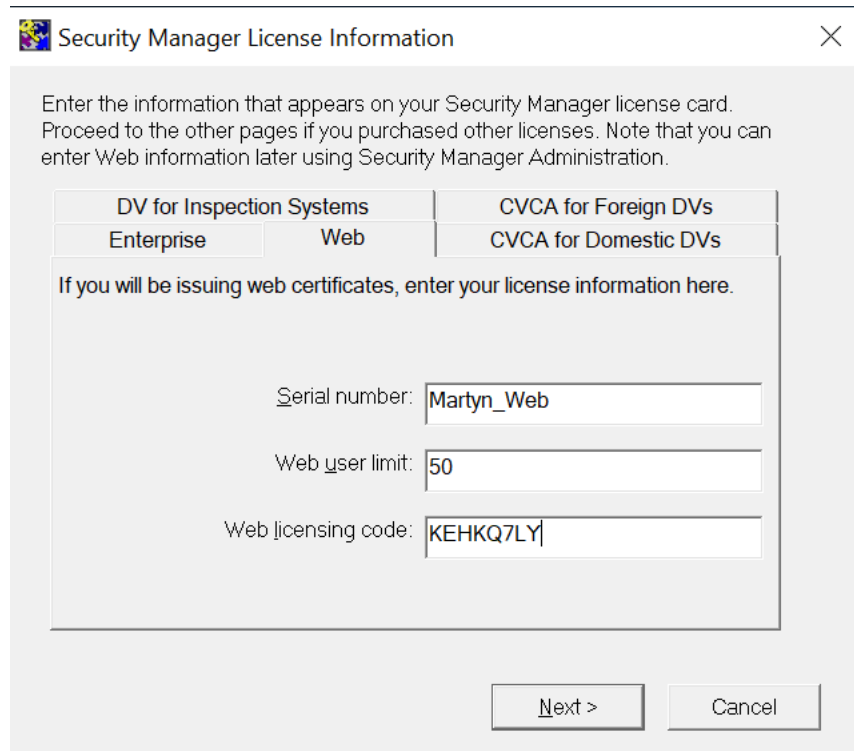
Welcome to the configuration program for Entrust Authority(TM) Security Manager. This program collects the information required to configure Security Manager to work with your Directory and Entrust-Ready applications.

Before you can run Security Manager Control Command Shell for the first time, you must complete this program.

Next >

Cancel

- 4 Next the license information screen appears. Enter the Enterprise license information from the `Training_SM_license_string.txt` file in the `Source\training licenses` folder. The **Enterprise** license information is required. Click **Next** to continue.



Security Manager License Information

Enter the information that appears on your Security Manager license card. Proceed to the other pages if you purchased other licenses. Note that you can enter Web information later using Security Manager Administration.

DV for Inspection Systems		CVCA for Foreign DVs
Enterprise	Web	CVCA for Domestic DVs

If you will be issuing web certificates, enter your license information here.

Serial number:

Web user limit:

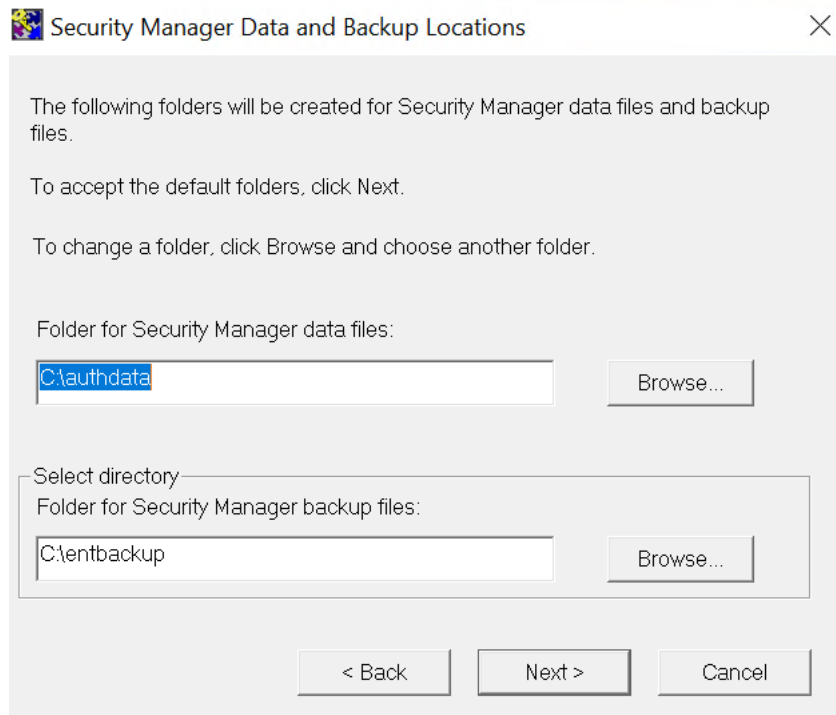
Web licensing code:



Note:

The **CVCA** tabs and the **DV for Inspection Systems** tab are mutually exclusive. For example, if Entrust Authority Security Manager is being configured as a CVCA, enter information into the CVCA tabs only. After the configuration is completed, license information can be added or changed in the `Security Manager Administration` application.

Enter the installation location for the Entrust Authority Security Manager data and backup files. Accept the default folder or click **Browse** to redirect to another location and click **Next**.



The following folders will be created for Security Manager data files and backup files.

To accept the default folders, click Next.

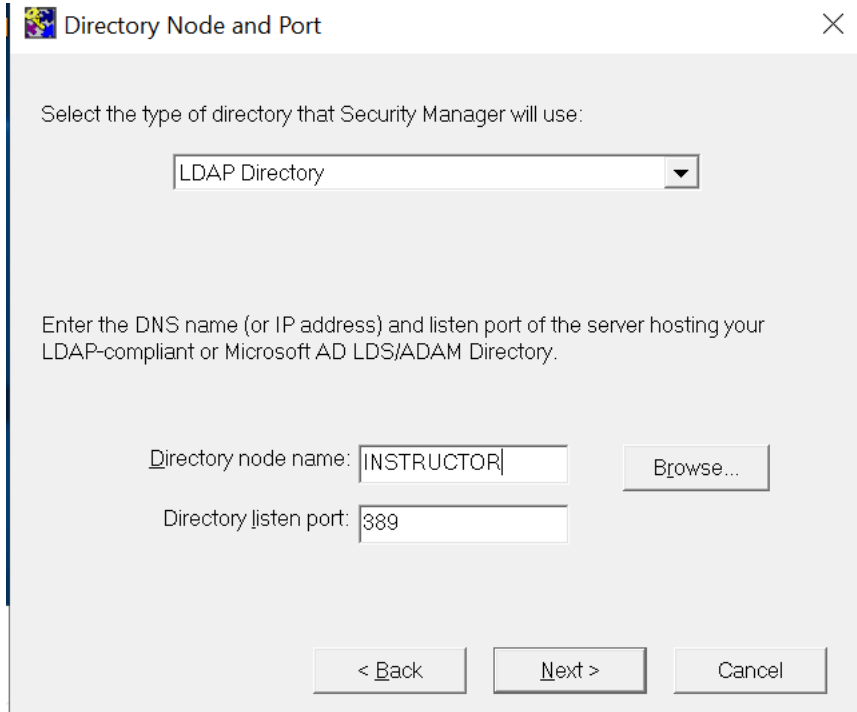
To change a folder, click Browse and choose another folder.

Folder for Security Manager data files:

Select directory

Folder for Security Manager backup files:

- 5 Select the type of Directory that will be used to store the public information published by Entrust Authority Security Manager. In the classroom, an LDAP Directory hosted on the **INSTRUCTOR** computer using port 389 will be used. Type these values and click **Next**.



Directory Node and Port

Select the type of directory that Security Manager will use:

LDAP Directory

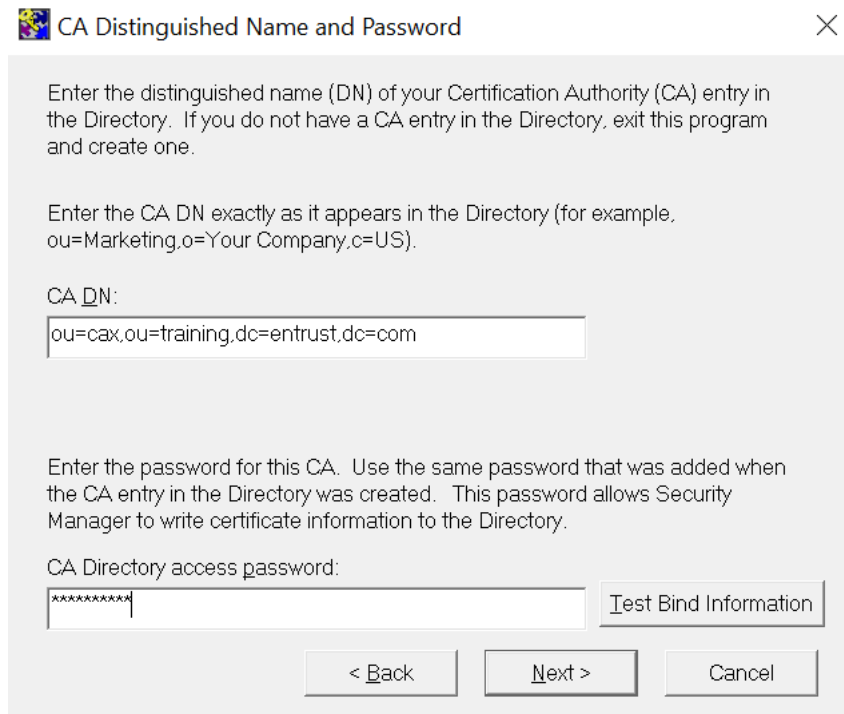
Enter the DNS name (or IP address) and listen port of the server hosting your LDAP-compliant or Microsoft AD LDS/ADAM Directory.

Directory node name: INSTRUCTOR Browse...

Directory listen port: 389

< Back Next > Cancel

- 6 The Certification Authority DN as well as the password that has been set for this entry in the Directory. This dialog box is presented during the configuration of Entrust Authority Security Manager when you are using a LDAP Directory.



The dialog box is titled "CA Distinguished Name and Password" with a close button (X) in the top right corner. It contains the following text and controls:

Enter the distinguished name (DN) of your Certification Authority (CA) entry in the Directory. If you do not have a CA entry in the Directory, exit this program and create one.

Enter the CA DN exactly as it appears in the Directory (for example, ou=Marketing,o=Your Company,c=US).

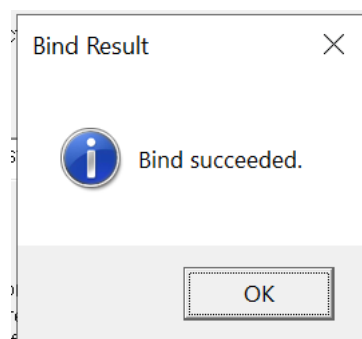
CA DN:

Enter the password for this CA. Use the same password that was added when the CA entry in the Directory was created. This password allows Security Manager to write certificate information to the Directory.

CA Directory access password:

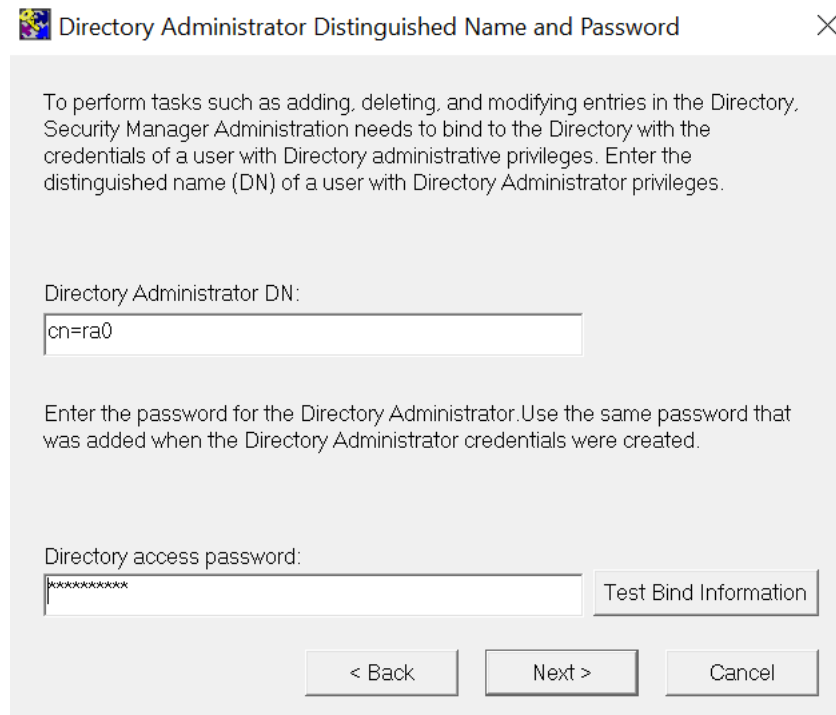
- **CA DN:** ou=CAX,ou=training,dc=entrust,dc=com
where x is your student number
- **CA Directory access password:** EntPKI2000 (entered when the Directory was installed)

Click **Test Bind Information** to insure a correct bind to the Directory is possible with the information provided.



Click **OK**, then **Next**.

- 7 Type the Directory Administrator DN as well as the password that has been set for that user in the Directory. These entries were set initially during the installation of the Directory.
- If using Microsoft Active Directory, this dialog box will not appear.



Directory Administrator Distinguished Name and Password

To perform tasks such as adding, deleting, and modifying entries in the Directory, Security Manager Administration needs to bind to the Directory with the credentials of a user with Directory administrative privileges. Enter the distinguished name (DN) of a user with Directory Administrator privileges.

Directory Administrator DN:
cn=ra0

Enter the password for the Directory Administrator. Use the same password that was added when the Directory Administrator credentials were created.

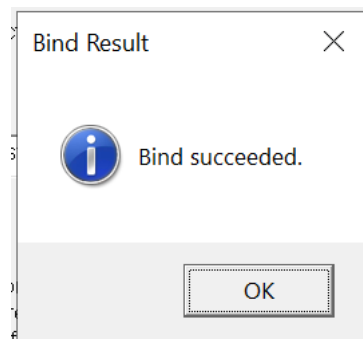
Directory access password:

Test Bind Information

< Back Next > Cancel

- **Directory Administrator DN:** cn=ra0
(All users in the classroom will be sharing the same Directory Administrator identity.)
- **CA Directory access password:** EntPKI2000 (entered when the Directory was installed)

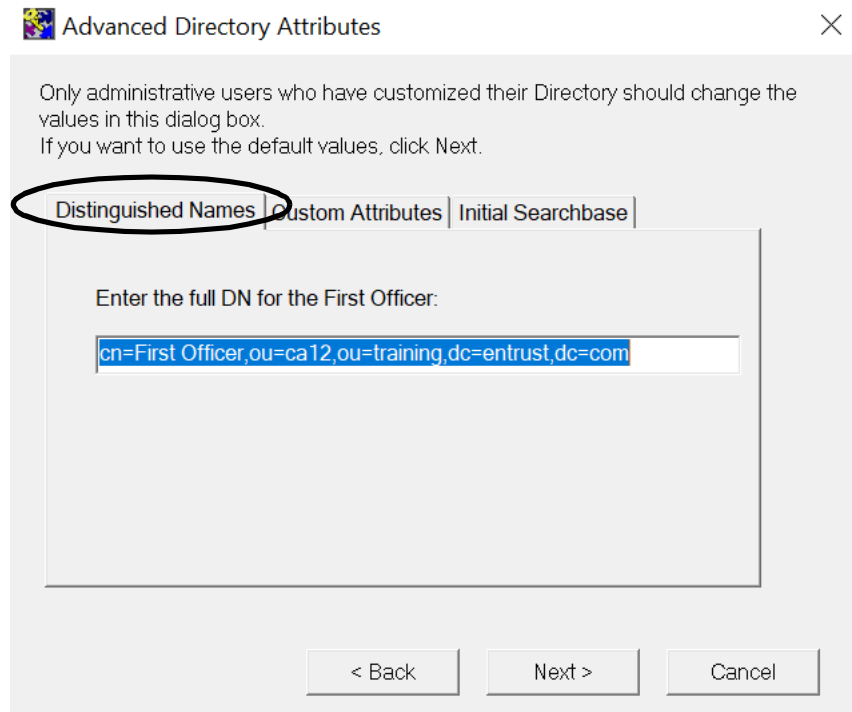
Click **Test Bind Information** to insure a correct bind to the Directory is possible with the information provided.



Click **OK**, then **Next**.

- 8 A tabbed dialog box will allow the selection of some Advanced Directory Attributes.

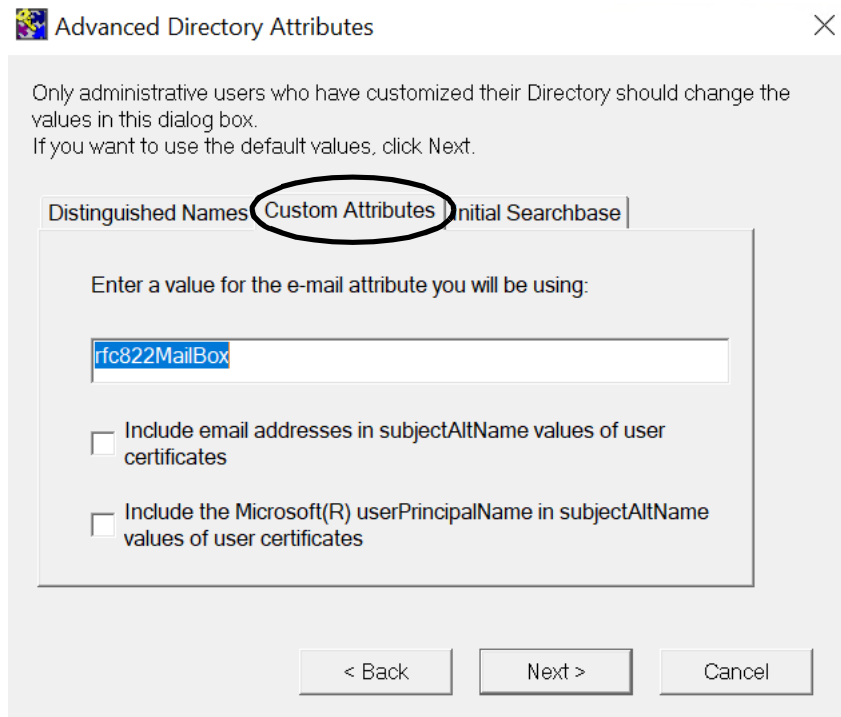
In some rare cases, the DN for the First Officer may need to be modified before initializing the Certification Authority. The **Distinguished Name** tab allows the DN of the First Officer to be changed.



The image shows a Windows-style dialog box titled "Advanced Directory Attributes" with a close button (X) in the top right corner. The dialog contains instructional text: "Only administrative users who have customized their Directory should change the values in this dialog box. If you want to use the default values, click Next." Below this is a tabbed interface with three tabs: "Distinguished Names", "Custom Attributes", and "Initial Searchbase". The "Distinguished Names" tab is selected and circled in red. Inside this tab, there is a text prompt "Enter the full DN for the First Officer:" followed by a text input field containing the value "cn=First Officer,ou=ca12,ou=training,dc=entrust,dc=com". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

In the classroom there is no need to modify the DN of the First Officer.

The **Custom Attributes** tab will allow the addition of an e-mail attribute. Some S/MIME applications require the e-mail address to be contained in certificates. This tab allows the value used to store the email address entry in the Directory.



The image shows the 'Advanced Directory Attributes' dialog box with the 'Custom Attributes' tab selected. The dialog has three tabs: 'Distinguished Names', 'Custom Attributes', and 'Initial Searchbase'. The 'Custom Attributes' tab is active, showing instructions to enter a value for the e-mail attribute. A text box contains 'rfc822MailBox'. Below the text box are two unchecked checkboxes: 'Include email addresses in subjectAltName values of user certificates' and 'Include the Microsoft(R) userPrincipalName in subjectAltName values of user certificates'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Advanced Directory Attributes

Only administrative users who have customized their Directory should change the values in this dialog box.
If you want to use the default values, click Next.

Distinguished Names | **Custom Attributes** | Initial Searchbase

Enter a value for the e-mail attribute you will be using:

rfc822MailBox

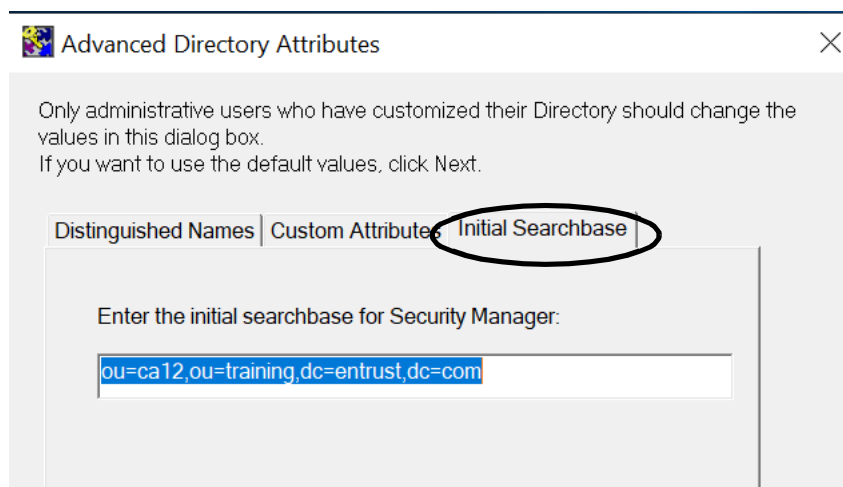
☐ Include email addresses in subjectAltName values of user certificates

☐ Include the Microsoft(R) userPrincipalName in subjectAltName values of user certificates

< Back Next > Cancel

- By default, most Directories use the mail attribute **rfc822MailBox**. Should the Directory use a different mail attribute, type that attribute name in the provided field
- Click **Include email addresses in subjectAltName values of user certificates** to include email addresses in the subjectAltName extension of user certificates
- If required, click **Include the Microsoft userPrincipalName in subjectAltName values of user certificates** to include the Microsoft userPrincipalName attribute value in the subjectAltName extension of user certificates (this is not required in the classroom)

The **Initial Searchbase** tab allows you to change the default searchbase before initializing Entrust Authority Security Manager (this is not required in the classroom).



The image shows the 'Advanced Directory Attributes' dialog box with the 'Initial Searchbase' tab selected. The dialog has three tabs: 'Distinguished Names', 'Custom Attributes', and 'Initial Searchbase'. The 'Initial Searchbase' tab is active, showing instructions to enter the initial searchbase for Security Manager. A text box contains 'ou=ca12,ou=training,dc=entrust,dc=com'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Advanced Directory Attributes

Only administrative users who have customized their Directory should change the values in this dialog box.
If you want to use the default values, click Next.

Distinguished Names | Custom Attributes | **Initial Searchbase**

Enter the initial searchbase for Security Manager:

ou=ca12,ou=training,dc=entrust,dc=com

< Back Next > Cancel

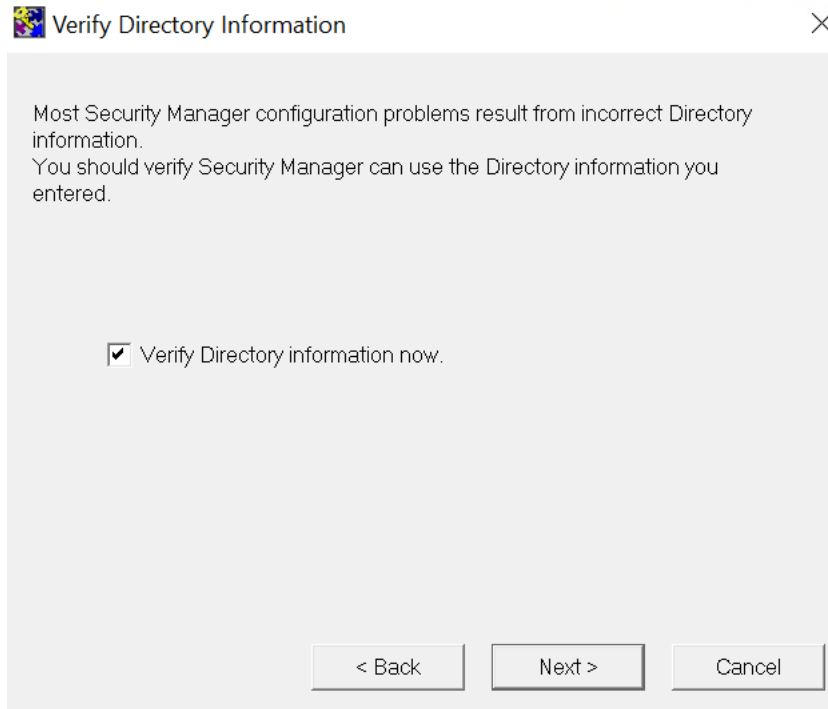


Note:

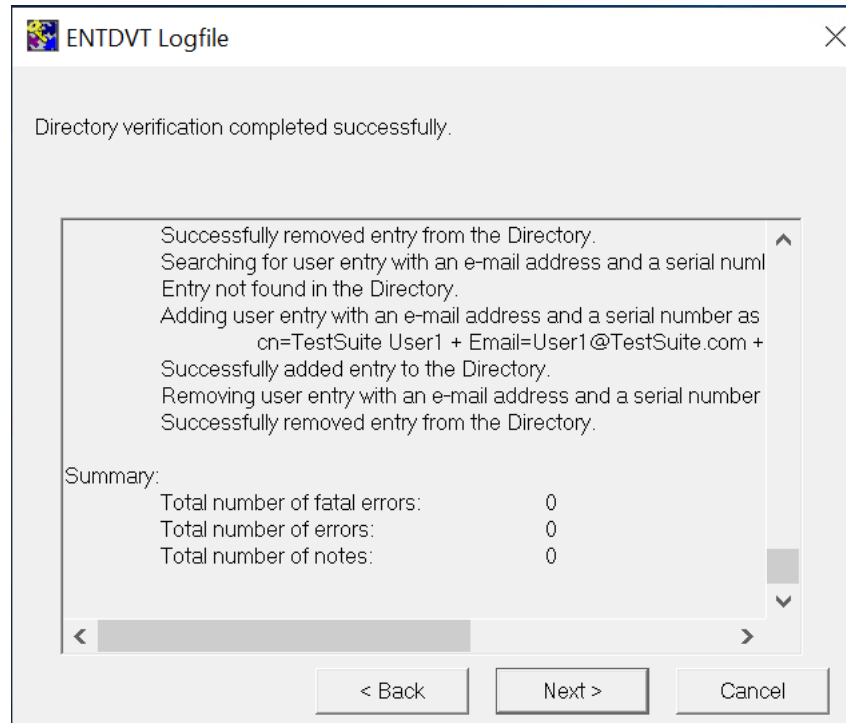
If using Active Directory, the default searchbase is the user container in the domain hosting Entrust Authority Security Manager (for example, `cn=Users,ou=training,dc=entrust,dc=com`)

Click **Next** to continue the configuration of Entrust Authority Security Manager.

- 9 The Directory information entered in the previous dialog boxes will be verified at this point. Insure **Verify Directory information now** is selected and click **Next**.



- 10 If any problems are reported, scroll through the displayed log information to locate the problem area, identified by the word **ERROR** in the list, and click **Back** to make the necessary changes.

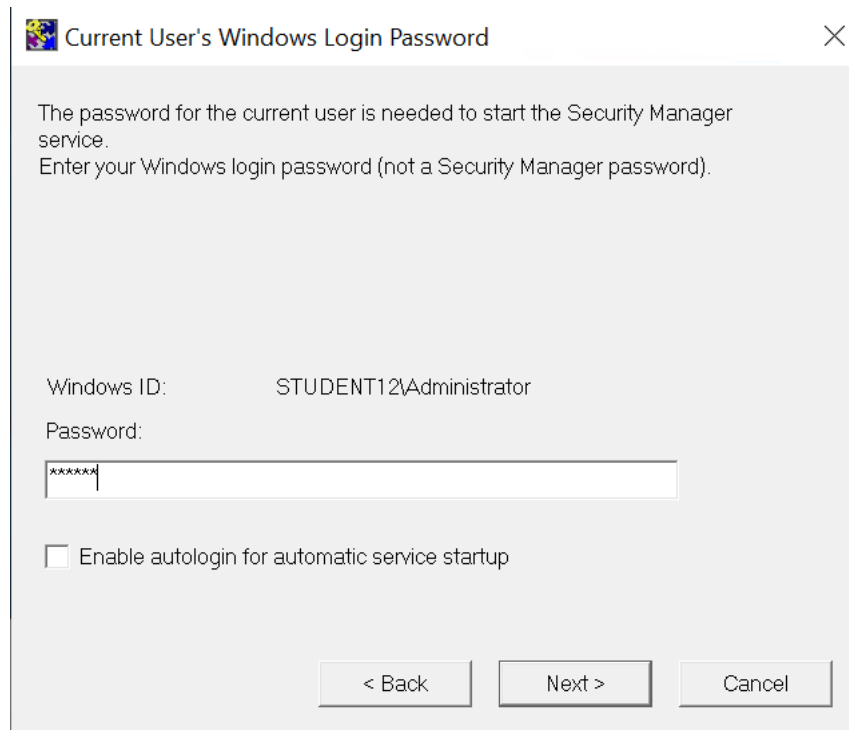


Note:

The Directory Verification Table is written to `entdvt.log` file located in `C:\Program Files\Entrust\Security Manager\etc\dvt`

Click **Next** when the Directory verification has completed successfully.

- 11 The Windows login password for the local administrator is required to start the Entrust Authority Security Manager service at the end of the configuration. Type the classroom password of Elmer1 (or type an alternate password indicated by the instructor) and click **Next**.



Current User's Windows Login Password

The password for the current user is needed to start the Security Manager service.
Enter your Windows login password (not a Security Manager password).

Windows ID: STUDENT12\Administrator

Password: *****

☐ Enable autologin for automatic service startup

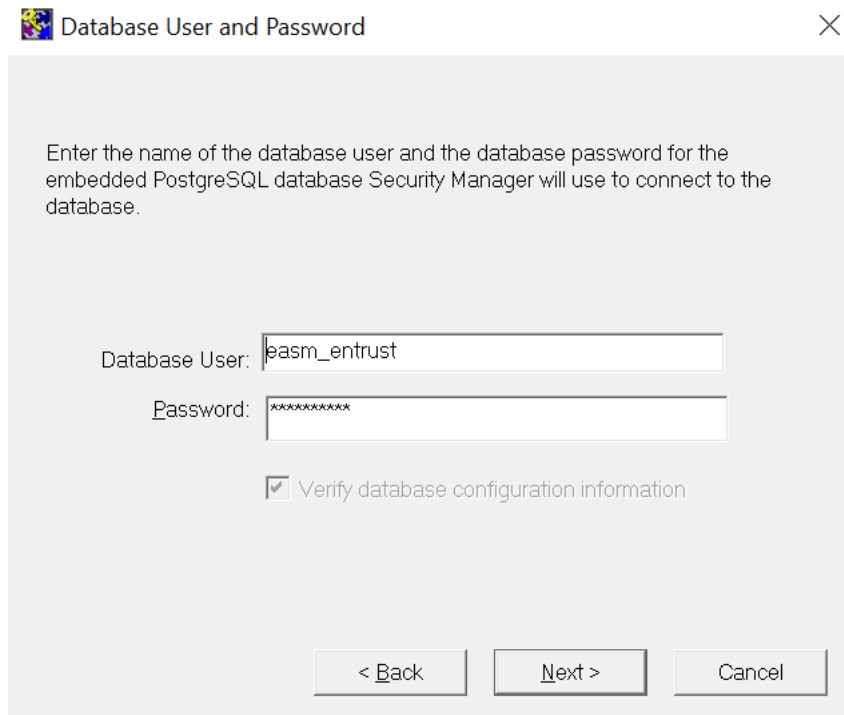
< Back Next > Cancel



Note:

The Entrust Authority Security Manager service is usually started manually by a Master User. By clicking **Enable autologin for automatic service startup** the Entrust Authority Security Manager service will be able to start automatically when the server is booted. This is not recommended.

- 12 Enter the password for the `easm_entrust` user in the database as `EntPKI2000` and click **Next**.



Database User and Password

Enter the name of the database user and the database password for the embedded PostgreSQL database Security Manager will use to connect to the database.

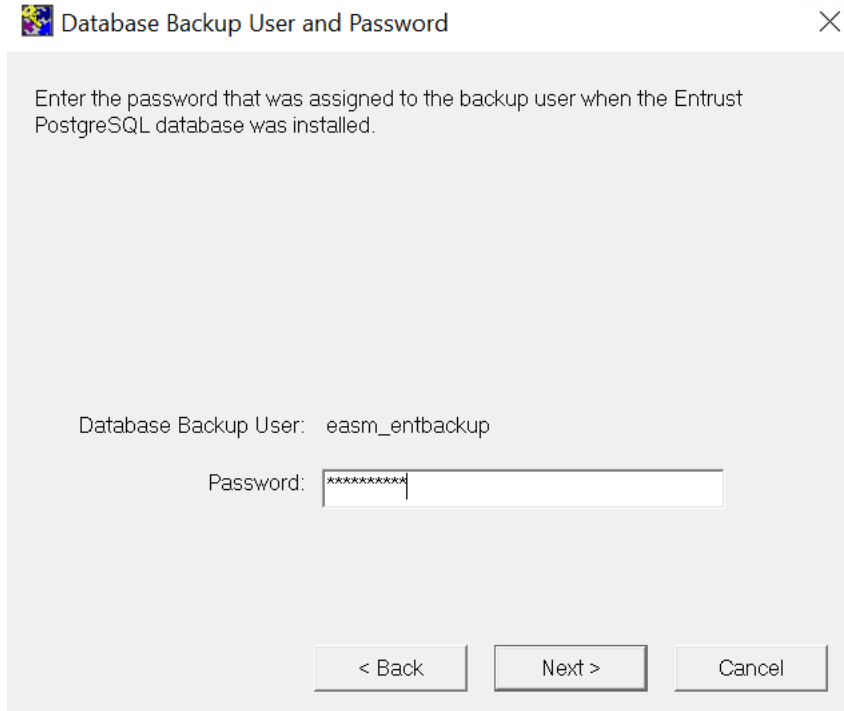
Database User:

Password:

☒ Verify database configuration information

< Back Next > Cancel

- 13 Enter the password for the `easm_entbackup` user in the database as `EntPKI2000` and click **Next**.



Database Backup User and Password

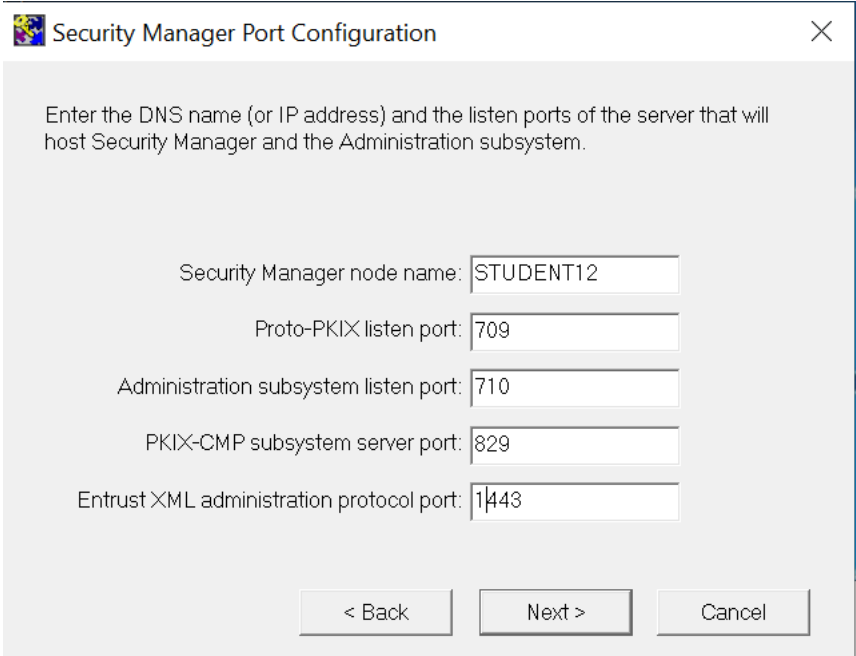
Enter the password that was assigned to the backup user when the Entrust PostgreSQL database was installed.

Database Backup User: `easm_entbackup`

Password:

< Back Next > Cancel

- 14 The server name of the computer hosting Entrust Authority Security Manager must be indicated in addition to the ports to be used for each subsystem. To avoid a possible port conflicts in the classroom, the **Entrust XML administration protocol port (XAP)** should be changed to 1443 as multiple applications may be installed on your classroom computer. (In a production environment this typically would not be an issue.) Click **Next**.



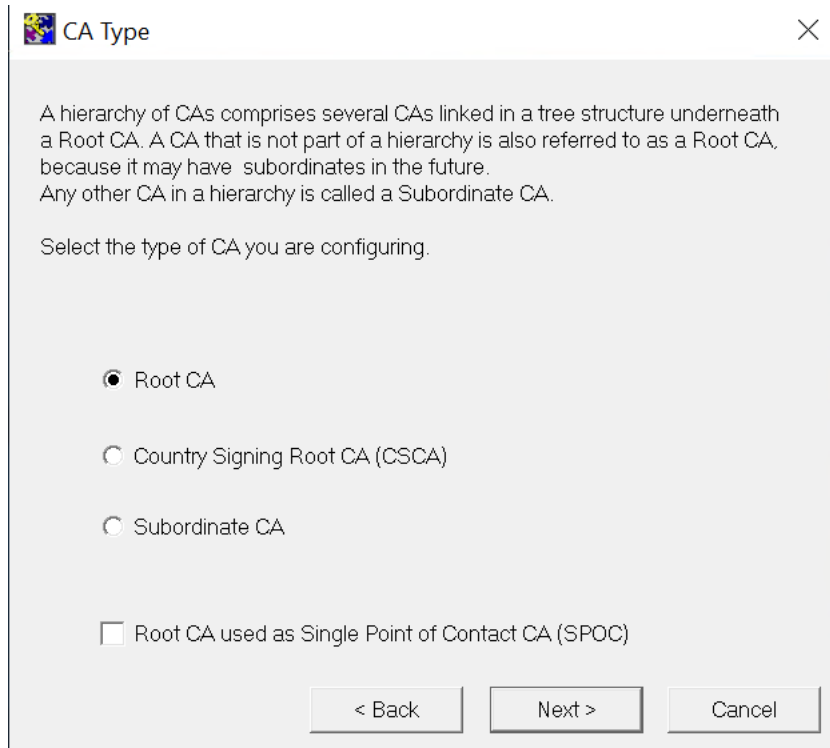
The image shows a Windows-style dialog box titled "Security Manager Port Configuration". It contains a text instruction at the top, followed by five input fields for configuration, and three buttons at the bottom.

Enter the DNS name (or IP address) and the listen ports of the server that will host Security Manager and the Administration subsystem.

Security Manager node name:	STUDENT12
Proto-PKIX listen port:	709
Administration subsystem listen port:	710
PKIX-CMP subsystem server port:	829
Entrust XML administration protocol port:	1443

< Back Next > Cancel

- 15 Since each Certification Authority in the classroom will operate as a root, click **Root CA** and click **Next**



The image shows a Windows-style dialog box titled "CA Type" with a close button (X) in the top right corner. The dialog contains a paragraph of text explaining the hierarchy of Certification Authorities (CAs). Below the text, there are three radio button options: "Root CA", "Country Signing Root CA (CSCA)", and "Subordinate CA". The "Root CA" option is selected. At the bottom, there is a checkbox labeled "Root CA used as Single Point of Contact CA (SPOC)" which is currently unchecked. At the very bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

CA Type

A hierarchy of CAs comprises several CAs linked in a tree structure underneath a Root CA. A CA that is not part of a hierarchy is also referred to as a Root CA, because it may have subordinates in the future. Any other CA in a hierarchy is called a Subordinate CA.

Select the type of CA you are configuring.

☒ Root CA

☐ Country Signing Root CA (CSCA)

☐ Subordinate CA

☐ Root CA used as Single Point of Contact CA (SPOC)

< Back Next > Cancel

- 16** The **Cryptographic Information** dialog box contains seven tabs to set the various policy settings for Security Manager and end users. Accept the default selections on each tab and click **Next**.

The figure displays six sequential screenshots of the 'Cryptographic Information' dialog box, showing the configuration steps for Security Manager and end users. Each screenshot shows a different tab selected, with the 'Next >' button highlighted in each.

- CA key generation:** The 'CA Signing Algorithm' tab is selected. The 'CA key generation' section shows 'Use software' selected and 'Use hardware' unselected.
- CA key pair type:** The 'CA Signing Algorithm' tab is selected. The 'CA key pair type' section shows 'RSA' selected, 'DSA' unselected, and 'EC' unselected. The 'Parameters' dropdown is set to '2048'.
- Signature Algorithms:** The 'CA Signing Algorithm' tab is selected. The 'Signature Algorithms' list shows 'RSA-SHA1', 'RSA-SHA256', 'RSA-SHA384', 'RSA-SHA512', 'ECDSA-SHA1', 'ECDSA-SHA256', 'ECDSA-SHA384', and 'ECDSA-SHA512'. 'RSA-SHA256' is selected.
- Database encryption algorithm:** The 'Policy Certificate' tab is selected. The 'Database encryption algorithm' list shows 'AES-CBC-128', 'AES-CBC-256', 'AES-GCM-128', 'AES-GCM-256', and 'TRIPLEDES-CBC-192'. 'AES-CBC-256' is selected.
- Policy Certificate Lifetime:** The 'Policy Certificate' tab is selected. The 'Policy Certificate Lifetime' field is set to '30'.
- Signing and Nonrepudiation Keys:** The 'Policy Certificate' tab is selected. The 'Signing and Nonrepudiation Keys' section shows 'RSA' selected, 'DSA' unselected, and 'EC' unselected. The 'Parameters' dropdown is set to '2048'.

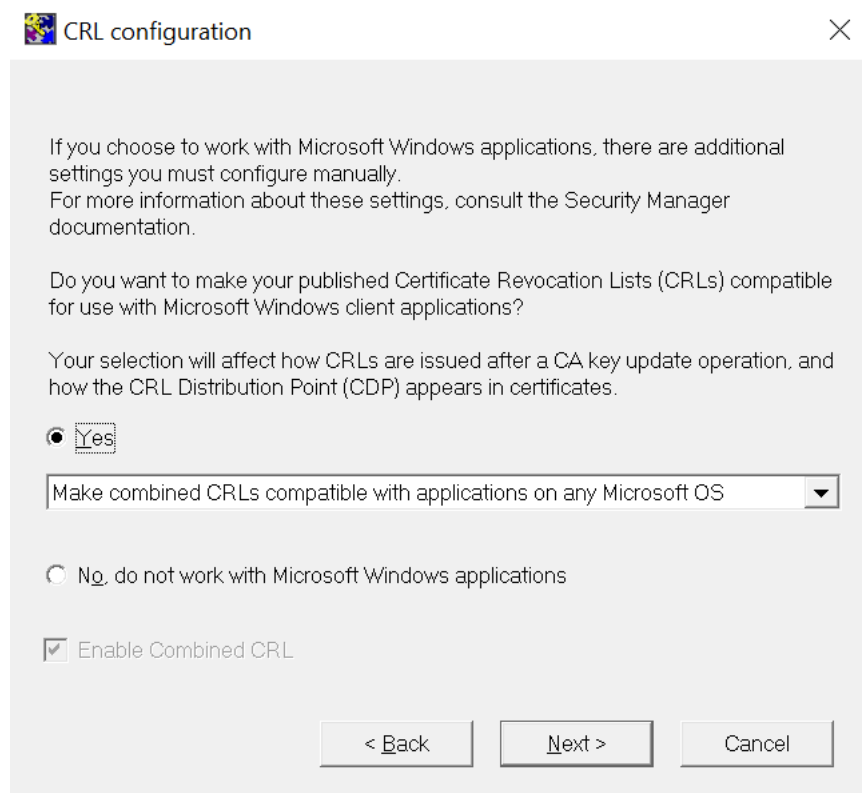


Note:

Ensure that the client software you will be using supports the algorithms you select. Not all clients support the algorithms listed here.

- 17 To insure compatibility of CRLs with Microsoft Windows client applications, combined CRLs must be enabled.

Click **Yes** and select **Make combined CRLs compatible with applications on any Microsoft OS**. Click **Next**.



CRL configuration

If you choose to work with Microsoft Windows applications, there are additional settings you must configure manually.
For more information about these settings, consult the Security Manager documentation.

Do you want to make your published Certificate Revocation Lists (CRLs) compatible for use with Microsoft Windows client applications?

Your selection will affect how CRLs are issued after a CA key update operation, and how the CRL Distribution Point (CDP) appears in certificates.

☒ **Yes**

Make combined CRLs compatible with applications on any Microsoft OS

☐ No, do not work with Microsoft Windows applications

☒ Enable Combined CRL

< Back Next > Cancel

- 18 The CRL Distribution Point (CDP) extension will be written into each certificate issued by the Entrust Authority Security Manager. By default, the revocation information used by Entrust clients will be stored in the Directory, but other locations can also be indicated, for example, for Microsoft clients. In this dialog, a choice of protocol and alternate location can be indicated.
- Combined CRL: This option will publish the CRL to the specified network location
 - Partitioned CRL: This option will publish the CRL to the specified network location
 - **URL Type:** This option will specify the type of URL to use in the CDP. The choices are `http`, `ldap`, `file`, `ftp`
 - **URL Host:** This option will specify the hostname to use in the CDP URL
 - **CDP Definition:** This option allows you to enter a CDP definition to include in certificates. It can be created from the settings above using the **Create from Settings** button, or it can be typed in the text box. Clicking **Add** then adds it to the list of default CDP URLs.

- **Default CDP URLs:** This field displays a list of CDP URLs that will be included in certificates.

CRL Distribution Point Information

Shared network CRL folders. Use Change button to select an existing network share.
Combined CRL share is mandatory.
Partitioned CRL share is mandatory if partitioned URLs defined..

Combined CRL: ☐ Disable

Partitioned CRL: ☐ Disable

Define one or more URLs for the distribution points in the CDP extension in certificates.
The URL host needs to be accessible by the entity validating the certificate.

URL Type: ▼

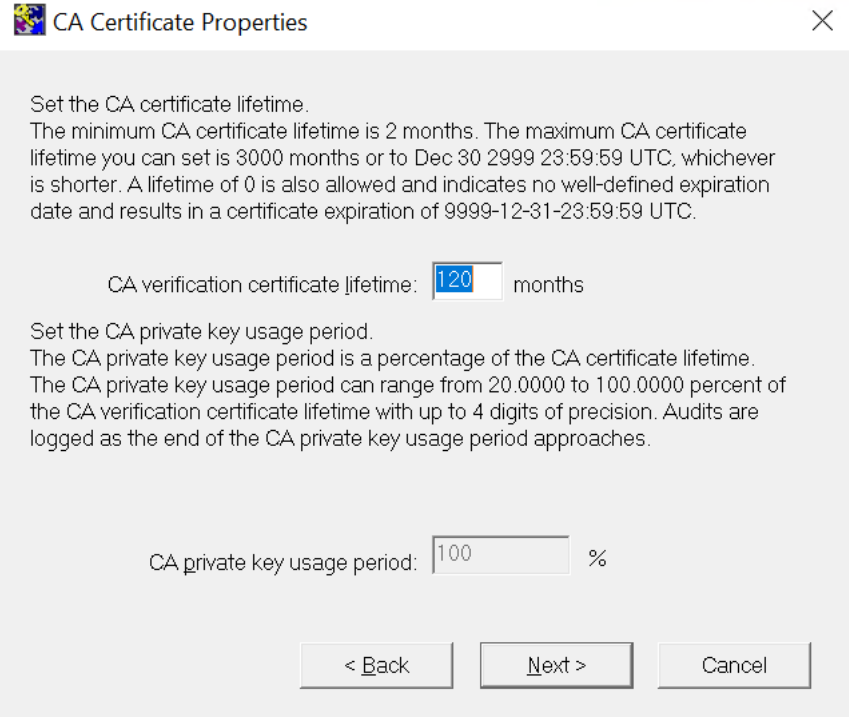
URL Host:

CDP Definition:

Default CDP URLs: ☒ Include LDAP DN ☒ LDAP DN Last

- 19 Leave the **URL Type** field set to `http` and enter the hostname for your machine into the **URL Host** field, for example, `CAX.training.entrust.com`.
- 20 Click **Create from Settings** to build the CDP URL.
- 21 Click **Add** to include it in the CDP extensions for user certificates.
- 22 Keep the checkbox selected to **Include LDAP DN**, and click **Next**.
- 23 The Certification Authority verification certificate lifetime as well as the private key usage period is indicated at this point. Since Microsoft compatibility for CRLs was enabled previously in the configuration process, the Certification Authority private key usage period is locked at 100%. This ensures that all certificates and CRLs are signed by the same Certification Authority, which is a requirement for Microsoft Windows client applications.

Accept the default verification certificate lifetime of 120 months and click **Next**.



CA Certificate Properties [X]

Set the CA certificate lifetime.
The minimum CA certificate lifetime is 2 months. The maximum CA certificate lifetime you can set is 3000 months or to Dec 30 2999 23:59:59 UTC, whichever is shorter. A lifetime of 0 is also allowed and indicates no well-defined expiration date and results in a certificate expiration of 9999-12-31-23:59:59 UTC.

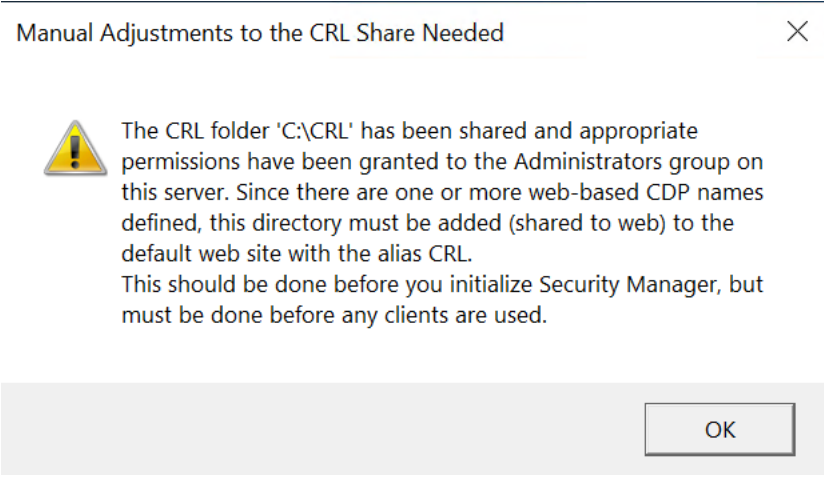
CA verification certificate lifetime: months

Set the CA private key usage period.
The CA private key usage period is a percentage of the CA certificate lifetime. The CA private key usage period can range from 20.0000 to 100.0000 percent of the CA verification certificate lifetime with up to 4 digits of precision. Audits are logged as the end of the CA private key usage period approaches.

CA private key usage period: %

< Back Next > Cancel

- 24 A message is displayed as a reminder that the appropriate share permissions must be set for the selected folder. Click **OK** to acknowledge the message.

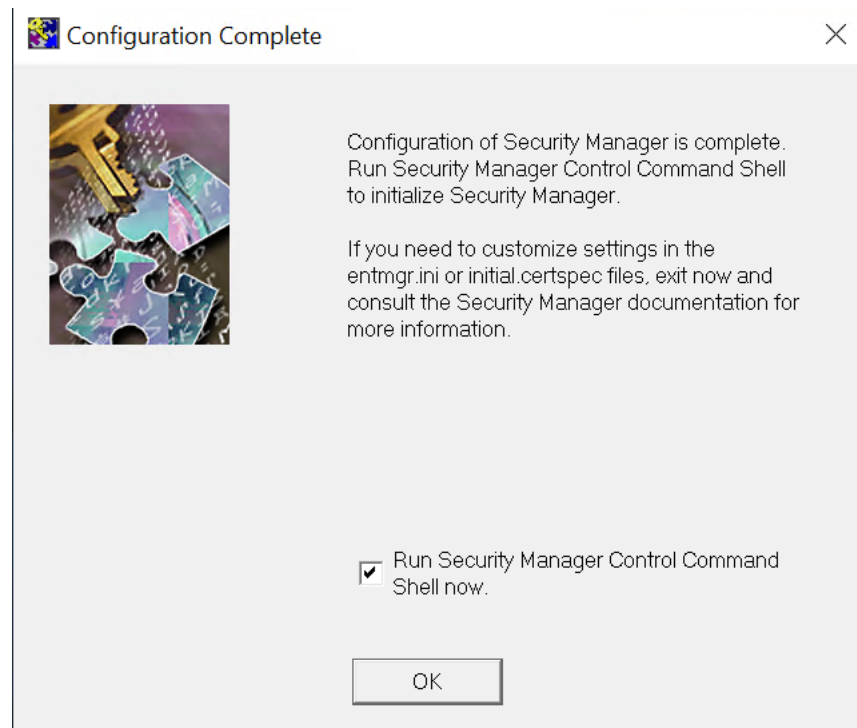


Manual Adjustments to the CRL Share Needed [X]

 The CRL folder 'C:\CRL' has been shared and appropriate permissions have been granted to the Administrators group on this server. Since there are one or more web-based CDP names defined, this directory must be added (shared to web) to the default web site with the alias CRL.
This should be done before you initialize Security Manager, but must be done before any clients are used.

OK

- 25 Once the configuration is complete, a confirmation dialog box is presented. Deselect **Run Security Manager Control Command Shell now** and click OK.



- 26 A message is displayed as a reminder that you can further customize settings - those from the wizard as well as additional settings - by editing the entmgr.ini and the initial.certspec files. Click **OK**.

At this point, the Certification Authority is configured, but does not yet possess a signing key pair. The initialization process will create the signing key pair and the identity of the first Security Officer.

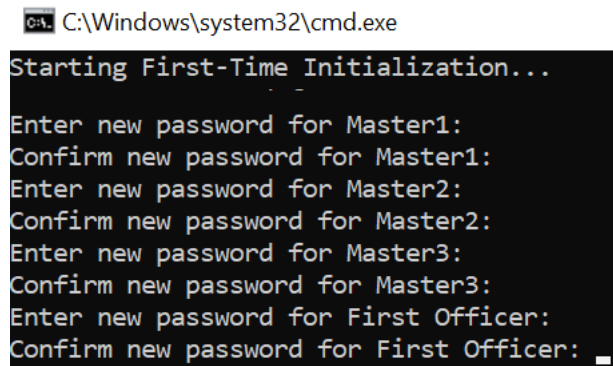
Exercise 4: Initialize Entrust Authority Security Manager

Entrust Authority Security Manager has been installed and configured. In this exercise, the Certification Authority will be initialized, which creates the signing key pair, the Master User accounts, the First Officer and Certification Authority security stores and performs the initial backup.

- 1 Click the **Security Manager Control Command Shell** shortcut on the desktop and at the command prompt, enter the following command to begin initialization:

```
init
```

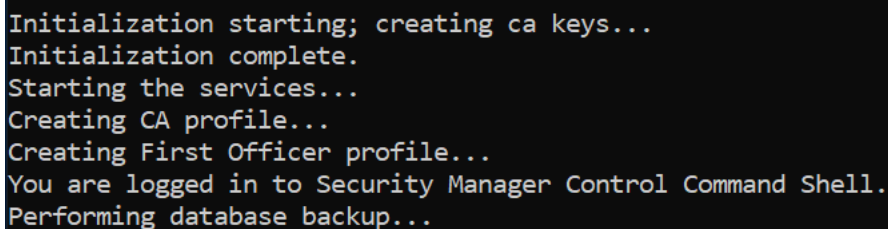
- 2 The Entrust Authority Security Manager Control Command Shell prompts Master User 1, Master User 2, Master User 3 along with the First Officer to type and confirm their password. (Type the classroom password of `EntPKI2000` for all the three Master User accounts and for the First Officer)



```
C:\Windows\system32\cmd.exe
Starting First-Time Initialization...
Enter new password for Master1:
Confirm new password for Master1:
Enter new password for Master2:
Confirm new password for Master2:
Enter new password for Master3:
Confirm new password for Master3:
Enter new password for First Officer:
Confirm new password for First Officer: _
```

After the passwords have been entered, the signing key pair, user key pair, and the First Officer security store are created and the services started.

- 3 The remaining initialization tasks will be performed including creating the CA profile and backup of the Database..



```
Initialization starting; creating ca keys...
Initialization complete.
Starting the services...
Creating CA profile...
Creating First Officer profile...
You are logged in to Security Manager Control Command Shell.
Performing database backup...
_
```

At this point Entrust Authority Security Manager has been initialized.

Discussion Questions

- 1 Why is the Certification Authority private key usage period fixed at 100% when Microsoft compatibility for CRLs is enabled?
- 2 What Directory-related information must be collected before Entrust Authority Security Manager is installed?
- 3 Before installing Entrust Authority Security Manager policy must be determined. What are some of the considerations before selecting the key lengths and algorithms of the Certification Authority key pair and users?

EASM Control Command Shell

In this lesson the Command Shell will be introduced as a management tool for Master Users.

Lab

In these exercises, participants will act as Master Users and execute command in the Security Manager Control Command Shell.

Tasks

The following tasks will be completed:

Exercise 1: Log into Security Manager Control Command Shell

Exercise 2: Viewing command help

Exercise 3: Work with Entrust Authority Security Manager services

Exercise 4: Enable multiple authorizations

Exercise 5: Adding custom Master Users

Exercise 6: Validate and backup the database

Exercise 7: Restore certificates to the Directory

Exercise 8: View Node information for clustering and generate Bootstrap information

Exercise 9: Importing and exporting key PKI information

Timing

Estimated time to complete these exercises is 20 minutes

Exercise 1: Log into Security Manager Control Command Shell

In this exercise, you will log into Entrust Authority Security Manager Control Command Shell as one of the three Master Users.

- 1 Click **Start > Apps > Entrust > Security Manager Control Command Shell**.
- 2 At the prompt, type the following command:
`login`
- 3 Entrust Authority Security Manager Control Command Shell prompts for the Master User name. Type the name of the Master User (for example, `Master1`) and press `<enter>`.



Note:

Master User names are case-sensitive.

- 4 Entrust Authority Security Manager Control Command Shell prompts for the Master User password. Type the password as entered when Entrust Authority Security Manager was initialized and press `<enter>`.

The prompt displays the Certification Authority DN and the Master User name.

The Master User is now logged in. Entrust Authority Security Manager Control Command Shell automatically logs the Master User out if there is no activity for five minutes.

Exercise 2: Viewing command help

In this exercise, the help command will be used to view the command structure.

- 1 Log into Entrust Authority Security Manager Control Command Shell, then type the following command:

```
help
```

or

```
?
```

 Security Manager Control Command Shell

```
Entrust Authority (TM) Security Manager Control Command Shell 10.0.0(609)
Copyright 1994-2020 Entrust. All rights reserved.
```

```
Type 'help' or '?' for help on commands
```

```
entsh$ login
```

```
Master User Name: Master1
```

```
Password:
```

```
You are logged in to Security Manager Control Command Shell.
```

```
ou=training,dc=entrust,dc=com.Master1 $ help
```

```
Type help <cmd> or <cmd> -help for syntax help
```

apropos	commands relating to regular expression
audit count	Query the number of audit records.
audit export	Export the audits from the database
audit export-history	Display audit exporting history.
audit export-verify	Verify the exported audit file(s)

A list of all the Entrust Authority Security Manager Control Command Shell commands appears, along with a brief description of what each command does. The commands are listed in alphabetical order.

- 2 To view help for specific command sets, type the following command:

```
help <CommandSetName>
```

(where <CommandSetName> is the name of the command sets as displayed in step 1)

For example, to get help for the **db** command set, type the following command:

```
help db
```

- 3 To view help for specific commands, type the following command:

```
help <CommandSetName><CommandName>
```

(where <CommandSetName> is the name of the command set as displayed in step 1 and

where <CommandName> refers to the name of the command)

For example, to get help on the command **db get**, type the following command:

```
help db get
```

Exercise 3: Work with Entrust Authority Security Manager services

In this exercise, the commands used to find out the current status of the Entrust Authority Security Manager subsystems will be executed, along with commands to stop and start the services.

- 1 Still logged in to Entrust Authority Security Manager Control Command Shell, type the following command:

```
service status
```

After a short interval, a list of all the Entrust Authority Security Manager subsystems and their current status appears, followed by the prompt.

```
ou=training,dc=entrust,dc=com.Master1 $ service status
Checking service status...
amb      Maintenance          enabled up    1 processes
ash      Admin Service Handler   enabled up    4 processes
backup   Automatic Backup           enabled up    1 processes
cmp      PKIX-CMP                   enabled up    2 processes
integ    Database Integrity Check   enabled up    1 processes
keygen   Key Generator              enabled up    1 processes
listen   Listener Service           enabled up    1 processes
rlsvc    Revocation List Service     enabled up    1 processes
sep      Entrust proto-PKIX          enabled up    2 processes
xap      XML Admin Protocol          enabled up    2 processes

ou=training,dc=entrust,dc=com.Master1 $ _
```

- 2 At the prompt, type the following command to start all the services and subsystems:

```
service start
```

After a short interval, the prompt re-appears and the Entrust Authority Security Manager services and subsystems have been started. If you need to stop the Entrust Authority Security Manager services at any time, type the command `service stop`.

- 3 Within Security Manager 10 multiple PKI nodes can be defined, use is the node command to identify how many nodes are present.

```
node list
```

```
ou=training,dc=entrust,dc=com.Master1 $ node list
NodeId LinkId          State    Version  Tzd        Label
0      N/A              enabled  10.0.0   UTC+00:00  ca_wide_entry
1      01D6-86F0-60F1-B0F2 enabled  10.0.0   UTC+00:00  instructor **LOCAL**
```

Notice the **NodeId** and the **label**.

- 4 By default, all subsystems are enabled when you start the Entrust Authority Security Manager service. Stopping the Entrust Authority Security Manager service disables all of its subsystems. You can choose to disable a subsystem that won't be used, for example, if the Enrollment Server or an older client application are not going to be used in your infrastructure, you may choose to disable the Entrust Secure Exchange Protocol subsystem. At the prompt, enter following command to view the status of the SEP subsystem on the current node (node 1):

```
service config -id 1 -subsys sep -query
```

A message appears, telling you whether the subsystem is enabled or disabled. The message also tells you the number of processes assigned to the subsystem.

- 5 To disable the SEP subsystem, type the following command:

```
service config -id 1 -subsys sep -disable
```

- 6 To re-enable the subsystem, type the following command:

```
service config -id 1 -subsys sep -enable
```

- 7 The number of processes dedicated to a subsystem can also be modified. To increase the number of processes dedicated to the ASH subsystem, type the following command:

```
service config -id 1 -subsys ash -procs 14
```

- 8 Type the following command once again to view the change to the subsystem:

```
service status
```

Exercise 4: Enable multiple authorizations

In this exercise, Entrust Authority Security Manager will be configured to require multiple authorizations to perform sensitive operations.

- 1 Still logged in to Entrust Authority Security Manager Control Command Shell type the following command:

```
policy auths enable
```

Multiple authorizations have now been enabled. Any sensitive operations will now require at least two Master Users to enter their password to complete the command.

- 2 Type the following command to change the password for another Master User, which is considered to be a sensitive operation:

```
passwd <Masterx>
```

(where <Masterx> is the name of a Master User other than the one currently logged in)

- 3 Since multiple authorizations are enabled, a second Master User will be required to enter their password to approve the operation. Enter and confirm the new Master User password.
- 4 The Master User who initiated the command will also be prompted to enter their password again to confirm the change

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ passwd Master2
Enter new password for Master2:
Confirm new password for Master2:
To confirm the change, enter the current password for Master1:
Password changed successfully.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ _
```

- 5 At the prompt, enter the following command to disable multiple authorizations:
- ```
policy auths disable
```
- 6 Confirm the change by entering the name of another Master User name and password.

## Exercise 5: Adding custom Master Users

In this exercise, a new Master User will be created and assigned a password.

- 1 Still logged into Entrust Authority Security Manager Control Command Shell, type the following command:

```
master add <username>
```

(where <username> is the name of the new Master User. The name can only contain printable ASCII letters (a-z, A-Z), numbers (0-9), and underscores (\_). The name cannot contain spaces.)

When Entrust Authority Security Manager prompts you to confirm the operation. Type **y** to confirm the operation.

- 2 Enter and confirm the password for the new Master User account.
- 3 If Entrust Authority Security Manager successfully creates the new Master User account, a confirmation message is displayed.

```
Security Manager Control Command Shell
Entrust Authority (TM) Security Manager Control Command Shell 10.0.0(609)
Copyright 1994-2020 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
entsh$ login
Master User Name: Master1
Password:
You are logged in to Security Manager Control Command Shell.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ master add nancy_crypto
Are you sure you want to add the new master user account nancy_crypto (y/n) ? [n] y
Enter new password for nancy_crypto:
Confirm new password for nancy_crypto:
Master user account nancy_crypto successfully added.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $
```

- 4 To display a list of all custom Master User accounts, type the following command:

```
master list
```

A list of all custom Master Users is displayed.

```
Master user account nancy_crypto successfully added.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ master list
nancy_crypto

ou=ca0,ou=training,dc=entrust,dc=com.Master1 $
```

## Exercise 6: Validate and backup the database

In this exercise, the database information will be validated and the backup schedule will be viewed. A manual backup will also be executed.

- 1 Still logged into Entrust Authority Security Manager Control Command Shell, type the following command to execute the database integrity check:

```
db integrity validate
```

A confirmation will be displayed when the procedure is complete

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ db integrity validate
100% complete. Estimated time remaining -:-:- -
Database integrity validation completed successfully.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ _
```

- 2 Type the following command to view the current database backup schedule and settings:

```
db backup query
```

The current backup schedule and settings will be displayed.

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ db backup query
backup-directory C:\entbackup
keep-online 7
incremental-backup-period 01:00
full-backup-period 24:00
not-before 03:00
not-after 05:00

ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ _
```

- 3 For execute a full backup, type the following command:

```
db backup full
```

A confirmation will be displayed when the backup is complete.

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ db backup full
NOTICE: pg_stop_backup complete, all required WAL segments have been archived
SUCCESS: Full backup completed successfully.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ _
```

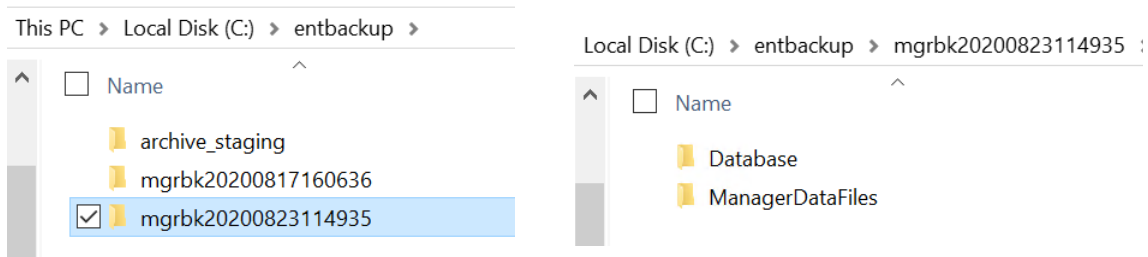
**Note:**

A database validation will be performed automatically before the database is backed up.

- 4 In Windows Explorer, browse to the following folder and view the folder in the current backup:

C:\entbackup

There will be backup folders named for the date and time when the backup occurred and there will be subfolders within each backup for the Database and the Manager Data Files.



## Exercise 7: Restore certificates to the Directory

In this exercise, Certification Authority and user certificates will be restored to the Directory.

- 1 Still logged in to Entrust Authority Security Manager Control Command Shell, type the following command to restore all the Certification Authority information to the Directory (policy certificate, revocation information, link certificates and cross certificates):

```
dsa restore ca
```

The Certification Authority information is refreshed in the Directory.

- 2 Type the following command to restore all public data, including user certificates, to the Directory

```
dsa restore all
```

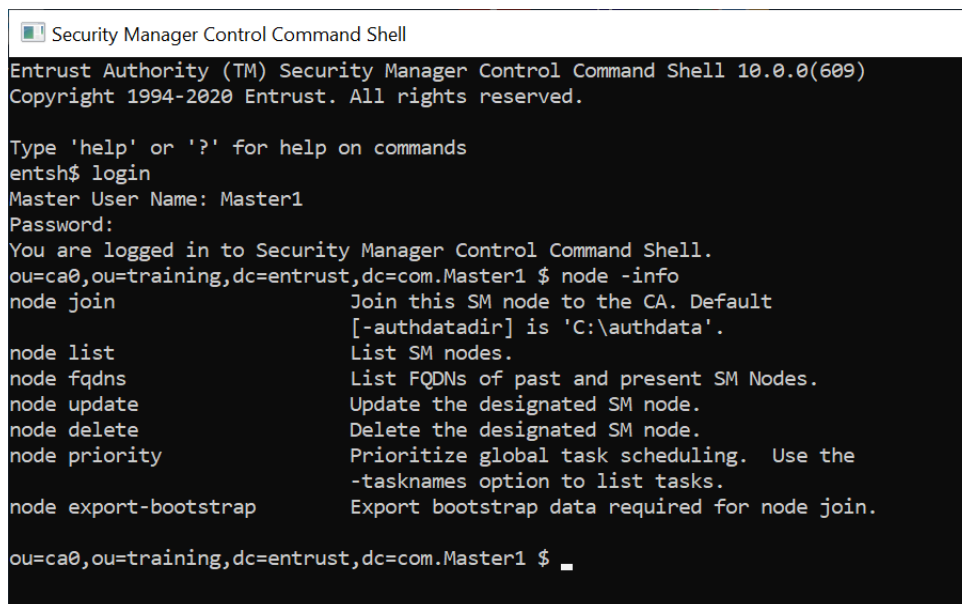
## Exercise 8: View Node information for clustering

In this exercise, the default node information setup at initialization will be viewed using the node commands introduced in SM10.

In SM10 PKIs can be clustered nodes all pointing to the same database. With a load balancer in front of the nodes this allows PKI maintenance on mission critical 24/7 systems. One node can be taken down for maintenance or even swapping and the other nodes will maintain connectivity with the Database.

- 1 Still logged into Entrust Authority Security Manager Control Command Shell type the following command:

```
node -info
```



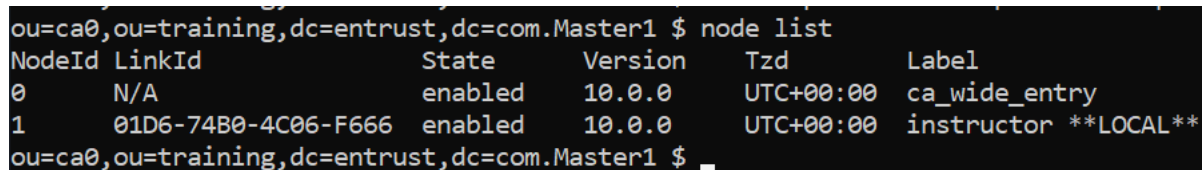
```
Security Manager Control Command Shell
Entrust Authority (TM) Security Manager Control Command Shell 10.0.0(609)
Copyright 1994-2020 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
entsh$ login
Master User Name: Master1
Password:
You are logged in to Security Manager Control Command Shell.
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ node -info
node join Join this SM node to the CA. Default
 [-authdatadir] is 'C:\authdata'.
node list List SM nodes.
node fqdns List FQDNs of past and present SM Nodes.
node update Update the designated SM node.
node delete Delete the designated SM node.
node priority Prioritize global task scheduling. Use the
 -tasknames option to list tasks.
node export-bootstrap Export bootstrap data required for node join.

ou=ca0,ou=training,dc=entrust,dc=com.Master1 $
```

- 2 To view the current node information type:

```
node list
```



```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ node list
NodeId LinkId State Version Tzd Label
0 N/A enabled 10.0.0 UTC+00:00 ca_wide_entry
1 01D6-74B0-4C06-F666 enabled 10.0.0 UTC+00:00 instructor **LOCAL**
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $
```

- 3 When we add a new node to the cluster we will need to use the bootstrap data from this the primary node for the configuration and initialization of the new node. This is done at install and we will practice this at the end of the course.

For now lets see how the bootstrap file is exported from this node type the command:

```
node export-bootstrap -bootstrapdir C:/authdata/bootstrap
```

- 4 In file explorer view the files in the directory above and note they were modified recently. We will come back to this later in the course when we do a new install and add it to the cluster as a new node.

## Exercise 9: Importing and exporting key PKI information

In this exercise we will import the entmgr information into the database. Then we can export it and share with other nodes if necessary.

- 1 Still logged into the command shell, type the following command **help config**.

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ help config
config disk-file Import or list on-disk configuration files.
config pwrules View and modify master user password rules.
config optional-file Manage optional on-disk files.
config entmgrini import Import CA-wide or node entmgr.ini.
config entmgrini export Export CA-wide or node entmgr.ini.

ou=ca0,ou=training,dc=entrust,dc=com.Master1 $
```

- 2 First we will do an export from the CA. This will allow us to save a copy or if required make any changes.
- 3 Type the following command  
config entmgrini export -ca -path /authdata/manager/entmgr.ini
- 4 Now, we can import the CA entmgr.ini file information to the node (-node 1) or CA wide (-ca).
- 5 Type the following command  
config entmgrini import -ca -path /authdata/manager/entmgr.ini

```
ou=ca0,ou=training,dc=entrust,dc=com.Master1 $ config entmgrini import -id 1 -path "C:/Program Files/Entrust/Security/Manager/etc/ini/entmgr.ini"

*** IMPORT SUMMARY: ***
Importing node data (NodeId:'1' LinkId:'01D6-74B0-4C96-F666' State:'enabled' Version:'10.0.0' Tzd:'UTC+00:00' Label:'instructor').
* Setting [login] 'maxProcs' with value '256' added.
 Setting [login] 'sepDisabled' with value 'false' added.
 Setting [login] 'cmpDisabled' with value 'false' added.
 Setting [login] 'ashDisabled' with value 'false' added.
 Setting [login] 'xapDisabled' with value 'false' added.
 Setting [login] 'backupDisabled' with value 'false' added.
 Setting [login] 'sepNumProcs' with value '2' added.
 Setting [login] 'cmpNumProcs' with value '2' added.
 Setting [login] 'ashNumProcs' with value '4' added.
 Setting [login] 'xapNumProcs' with value '2' added.
* Setting [login] 'watchdog' with value '300' added.
 Setting [login] 'maxRestarts' with value '10' added.
 Setting [logging] 'FileSize' with value '1024' added.
 Setting [logging] 'NumFiles' with value '5' added.
* = Services or cluster restart required.

Found 0 Warnings and 132 ERRORS:
[(-15274) Setting is system-wide only and cannot be specified for a single node.] INFO: New Setting [Comms]
'server' cannot be set for a single node. It is only allowed as a system wide setting.
[(-15274) Setting is system-wide only and cannot be specified for a single node.] INFO: New Setting [Comms]
'Mgrlisten' cannot be set for a single node. It is only allowed as a system wide setting.
```

- 6 This will load the file data into the CA database.

## Discussion Questions

- 1 Where is the security store of the Master User stored? How does the account for a Master User differ from the account of an administrative user or an end user?
- 2 What would happen if a single Master User forgot their password?  
What would happen if two Master Users forgot their passwords?  
What would happen if three Master Users forgot their passwords?
- 3 What is the purpose of the bootstrap information, how can it be used?

## Registering and activating administrative users in SMA (Security Manager Administration)

In this lesson the installation of the Administration tool, and its use to create and manage administrative users will be introduced.

## Lab

In these exercises, participants will register and activate digital IDs for administrative users.

### Tasks

The following tasks will be completed:

Exercise 1: Install Security Manager Administration

Exercise 2: Log into the Entrust Authority Security Manager Administration as the First Officer

Exercise 3: Register a new Security Officer

Exercise 4: Activate the Security Officer's digital ID

Exercise 5: Register and activate additional administrative users

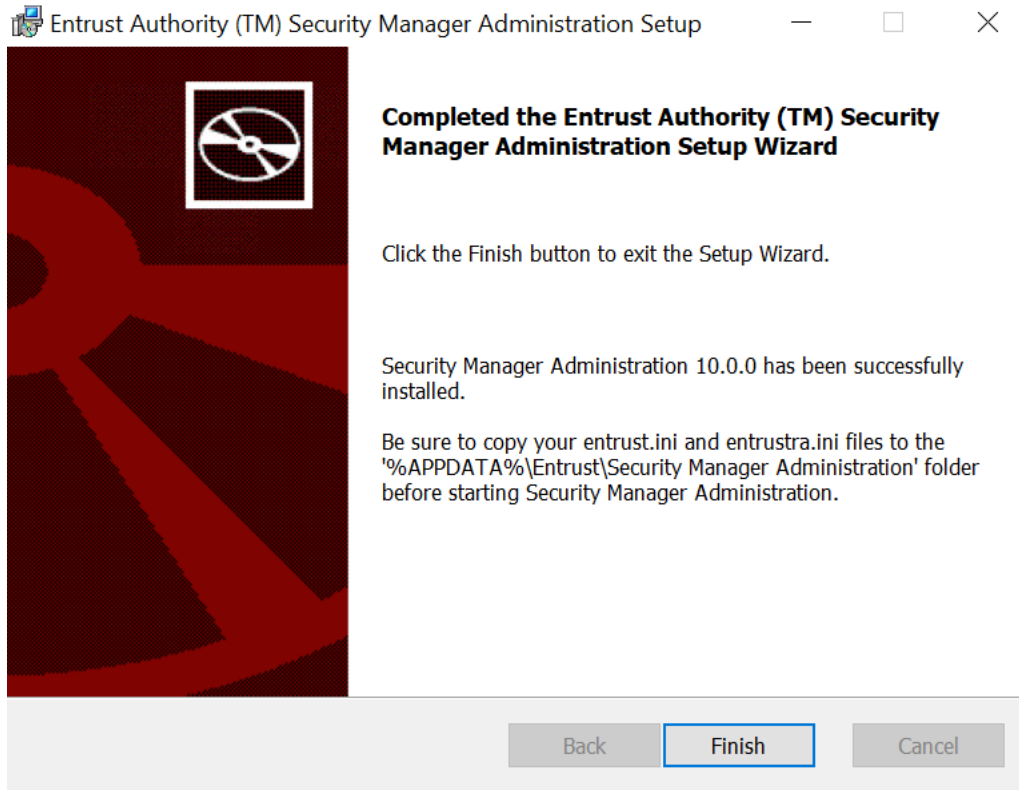
### Timing

Estimated time to complete these exercises is 30 minutes

## Exercise 1: Install Security Manager Administration

In this exercise, Security Manager Administration will be installed on your computer.

- 1 Locate and double-click the `SecurityManagerAdministration.10...` installation file from the `...\Source\SMA 10` folder (or an alternate location indicated by the instructor) to start the installation program. The files are extracted from the archive.



- 2 Click **Finish** to close the installation wizard.

Next the client\_entrust.ini and the entrustra.ini must be copied from **C:\authdata\optional** folder to **C:\Users\Administrator\AppData\Roaming\Entrust\Security Manager Administration** folder

- 3 Rename the client\_entrust.ini to entrust.ini.



**Note:**

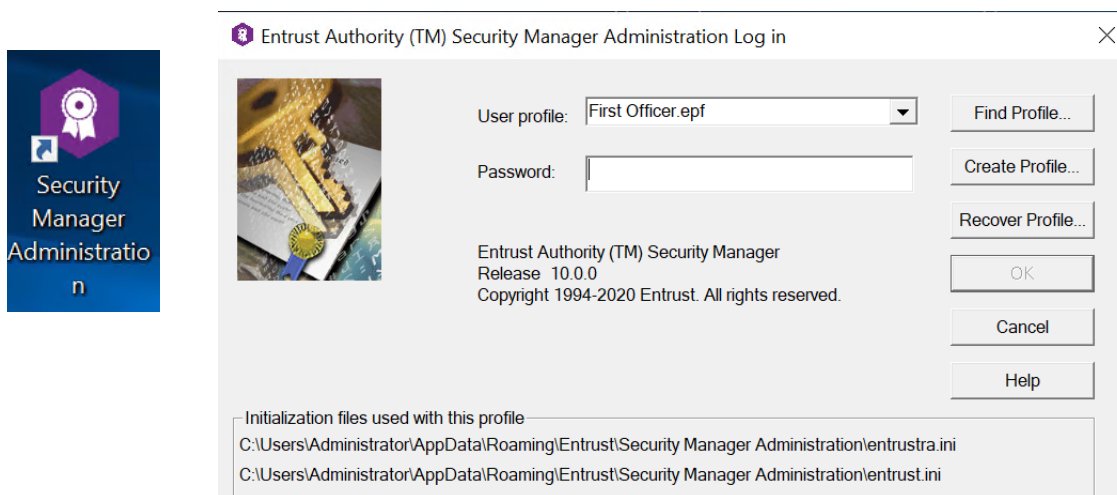
The destination folder is not visible through explorer. To open a window with the folder visible - First open an explorer window then type the path to the location

| C:\Users\Administrator\AppData\Roaming\Entrust\Security Manager Administration              |                  |                      |
|---------------------------------------------------------------------------------------------|------------------|----------------------|
| <input type="checkbox"/> Name                                                               | Date modified    | Type                 |
|  entrust   | 9/9/2020 9:30 PM | Configuration settin |
|  entrustra | 9/9/2020 9:30 PM | Configuration settin |

## Exercise 2: Log into the Entrust Authority Security Manager Administration as the First Officer

Currently, the First Officer is the only identity that can log in to Entrust Authority Security Manager Administration as their digital ID (stored in a desktop security store) was created during the initialization of Entrust Authority Security Manager. In this exercise, you will log in as the First Officer.

- 1 Double-click the **Security Manager Administration** icon on the desktop or click **Start > Apps > Entrust > Security Manager Administration**.



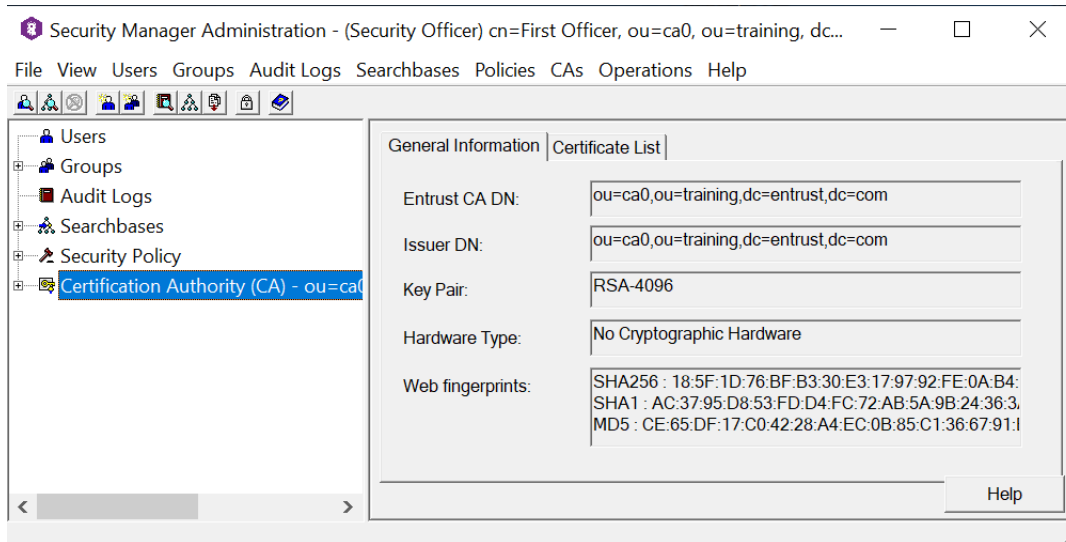
- 2 In the **Security Manager Administration Log in** window, type the password set by the First Officer when Entrust Authority Security Manager was initialized, for example `EntPKI2000`, and click **OK**.



### Note:

Entrust Authority Security Manager Administration will look for the `First Officer.epf` file in the `C:\authdata\manager\epf` folder. If the file is located elsewhere, click **Find Profile** to redirect to another location.

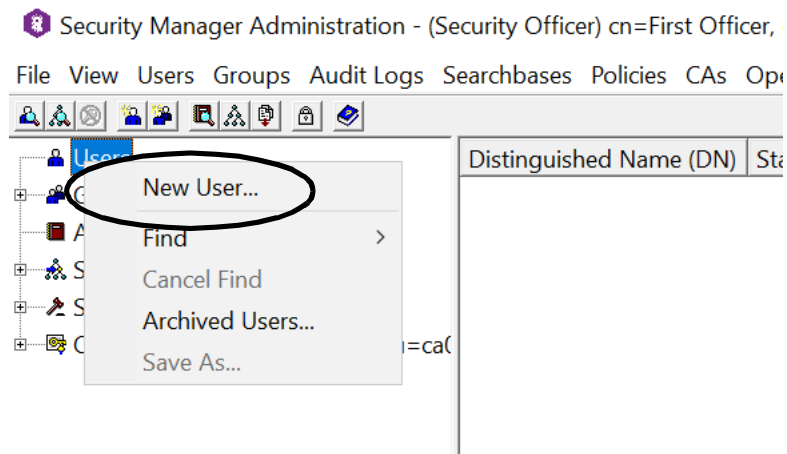
### 3 Entrust Authority Security Manager Administration is displayed.



## Exercise 3: Register a new Security Officer

In this exercise, the First Officer (with the role of Security Officer) will register another Security Officer.

- 1 Logged in to Entrust Authority Security Manager Administration as the First Officer, right-click the **User** icon in the left hand pane and click **New User**.



Alternately, click **Users > New User**, or click the **New User** on the toolbar.



### Note:

The **New User** option is not available for implementations using Microsoft Active Directory.

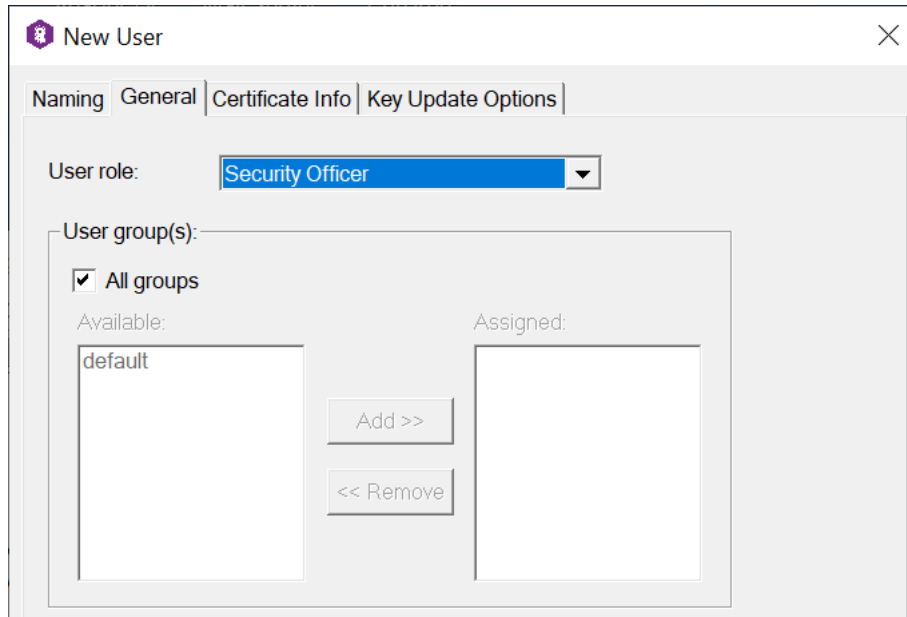
- 2 The **New User** dialog box is displayed. On the **Naming** tab, enter the identification information for the new Security Officer.

The screenshot shows the 'New User' dialog box with the 'Naming' tab selected. The 'Type' dropdown is set to 'Person'. Below it, a text box contains the message: 'This is the user type to be used for most Entrust users.' The 'In DN' section has four rows: 'First Name' (checked), 'Last Name' (unchecked), 'Serial Number' (unchecked), and 'Email' (unchecked). Below this, a note states: 'Asterisks (\*) appear beside required attributes.' The 'Add to:' dropdown is set to 'CA Domain Searchbase'. There is a 'Show DN...' button and a 'Create profile' checkbox at the bottom.

|               | In DN                               |
|---------------|-------------------------------------|
| * First Name  | <input checked="" type="checkbox"/> |
| * Last Name   | <input type="checkbox"/>            |
| Serial Number | <input type="checkbox"/>            |
| Email         | <input type="checkbox"/>            |

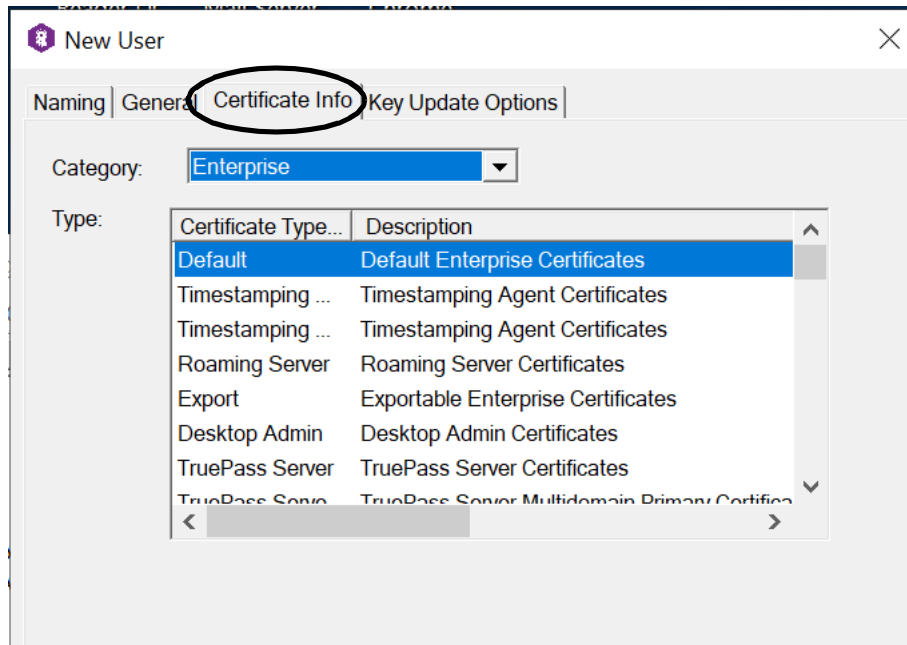
- **Type:** As the Security Officer is a human being, as opposed to a device, select the **Person** template
- **First Name** and **Last Name:** Type the name for the new Security Officer
- **Serial Number:** If multiple users have the same name, or an additional element of uniqueness for the user, type a serial number for the user. Click **In DN** to add the serial number to the distinguished name of the user  
Click **Show DN** to display the distinguished name that is created based on the information provided.
- **Add to:** Leave the searchbase as the default of **CA Domain Searchbase**

- 3 On the **General** tab, select a role and group for your new administrative user.



The screenshot shows the 'New User' dialog box with the 'General' tab selected. The 'User role' dropdown is set to 'Security Officer'. Under 'User group(s)', the 'All groups' checkbox is checked. The 'Available' list contains 'default', and the 'Assigned' list is empty. 'Add >>' and '<< Remove' buttons are between the lists.

- **User role:** Select the role of **Security Officer** from the list
  - **User group(s):** Ensure that **All groups** is selected. This will add the Security Officer to all existing groups and any new groups that are created at a later date
- 4 On the **Certificate Info** tab assign a certificate type to the new Security Officer.



The screenshot shows the 'New User' dialog box with the 'Certificate Info' tab selected. The 'Category' dropdown is set to 'Enterprise'. The 'Type' dropdown is open, showing a list of certificate types with 'Default' selected.

| Certificate Type... | Description                                      |
|---------------------|--------------------------------------------------|
| Default             | Default Enterprise Certificates                  |
| Timestamping ...    | Timestamping Agent Certificates                  |
| Timestamping ...    | Timestamping Agent Certificates                  |
| Roaming Server      | Roaming Server Certificates                      |
| Export              | Exportable Enterprise Certificates               |
| Desktop Admin       | Desktop Admin Certificates                       |
| TruePass Server     | TruePass Server Certificates                     |
| TruePass Sona       | TruePass Server Multidomain Primary Certificates |

- **Category:** Select the **Enterprise** category.
- **Type:** Since the Security Officer profile will be activated using Entrust Authority Security Manager Administration, click the certificate type of **Default**.

**Note:**

Entrust Authority Security Manager Administration does not understand the concept of certificate definition policies; digital IDs activated from this application will contain keys and certificates generated based on the default certificate policies and will be stored in a desktop security store and will be identified as V1 . Digital IDs activated using Entrust Security Provider will create keys and certificates based on certificate definitions policies and be V2.

- 5 The **Key Update Options** tab allows a Security Officer to override the default key update policy values. No changes are required for this exercise.

New User

Naming | General | Certificate Info | **Key Update Options**

Category currently selected: Enterprise

☒ Use default key update policy

Key update policy

☒ Set key lifetimes  
☐ Set key expiry

Key lifetimes

Key will be updated automatically for Enterprise certificate

Encryption public key lifetime: 36 months  
Verification public key lifetime: 36 months  
Private key usage period: 70 % of verification key lifetime

Key expiry

Encryption public and signing private keys expire on: 8/24/2020 1:22:25 AM  
Verification public key expires on: 8/24/2020 1:22:25 AM

- 6 Click **OK** to register the user with the selected parameters.
- 7 Authorize this activity by entering the password for the First Officer.

Authorization Required

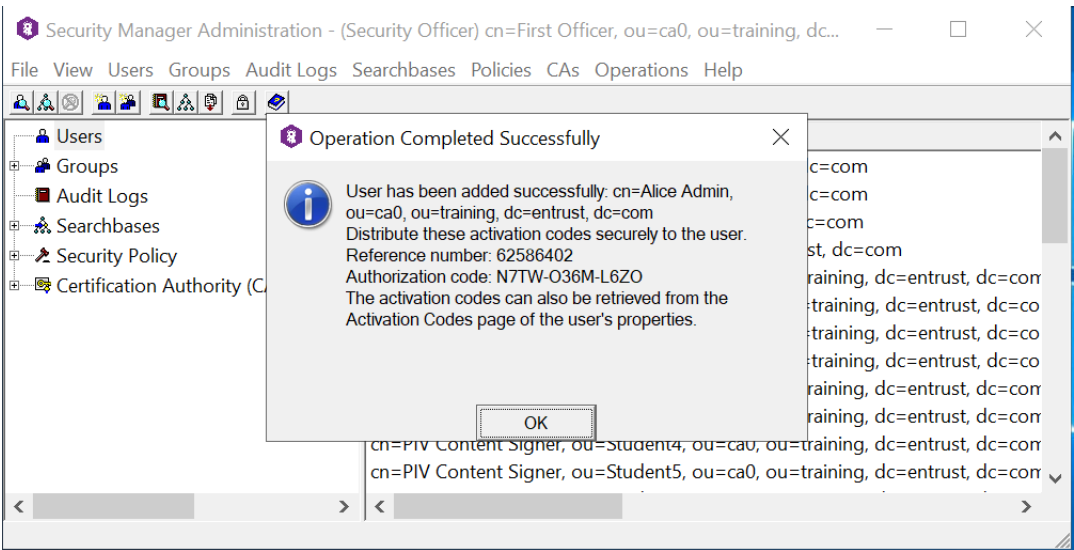
Authorization is required to add a user to Entrust.

Please enter the password for  
First Officer.epf

Password:

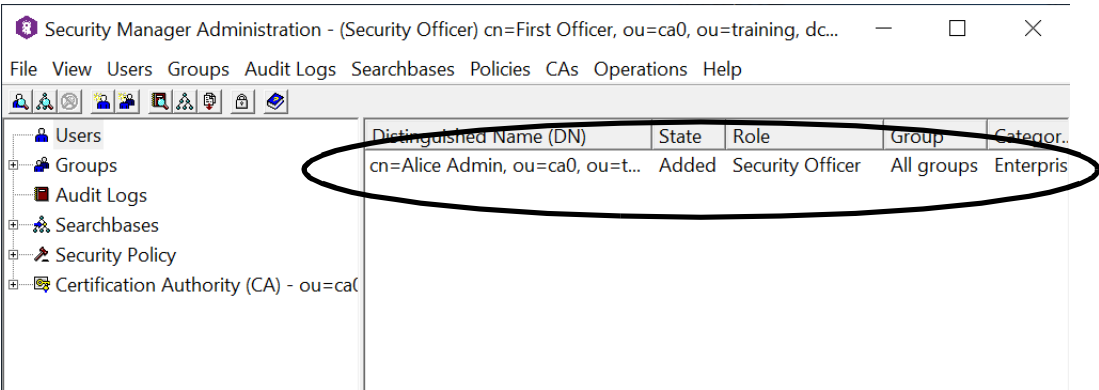
OK Cancel Help

The user registration is confirmed. A **Reference Number** and **Authorization Code** for the user is displayed. These codes will be required when the Security Officer profile is activated.



Record these on your user planning worksheet for later use.

- 8 Click **Users** in the left pane of the Entrust Authority Security Manager Administration. The newly-registered user will be listed in the right-hand pane of the window.



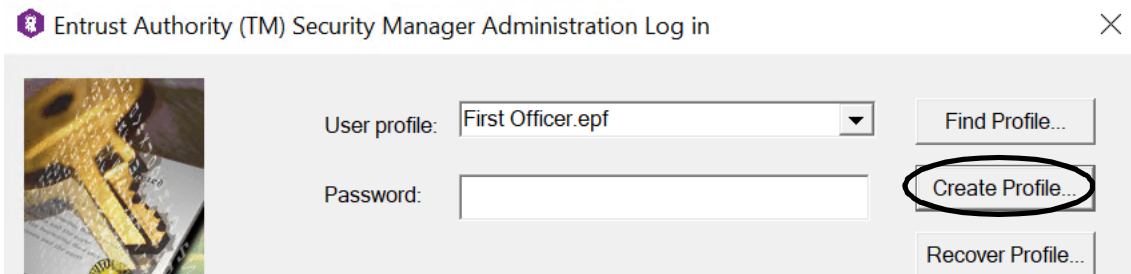
The user state is listed as **Added**.

- 9 Close Entrust Authority Security Manager Administration. The registration of the new Security Officer is complete.

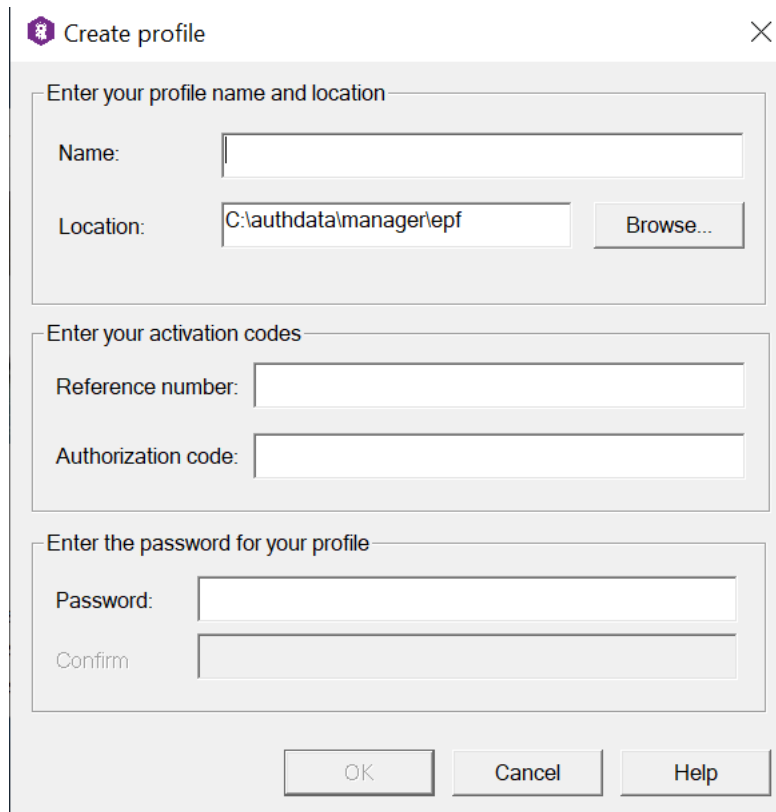
## Exercise 4: Activate the Security Officer's digital ID

In this exercise, a digital ID and a desktop security store will be activated for the new Security Officer. The **Reference Number** and **Authorization Code** that were generated when the new Security Officer was registered in Entrust Authority Security Manager Administration are required to complete this operation.

- 1 Double-click the **Security Manager Administration** icon on the desktop or click **Start > Apps > Entrust > Security Manager Administration**.
- 2 In the **Entrust Authority Security Manager Administration Log in** dialog box, click **Create Profile**.



- 3 Enter the details of the Security Officer profile as required.

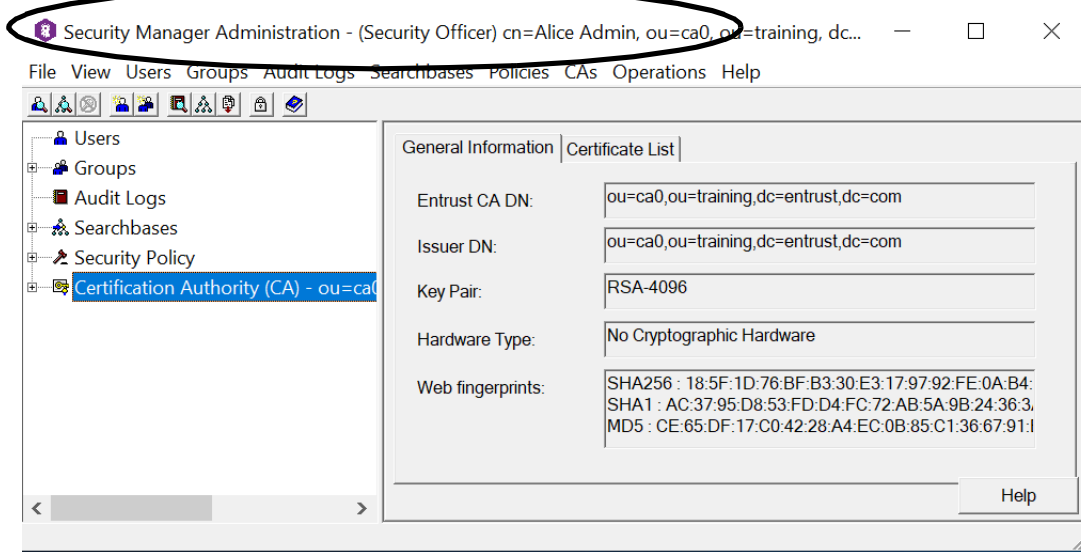


- **Name:** In this field enter the name for the security store. This name will be used to create the desktop security store file, an .epf extension will be added
- **Location:** Accept the default location for the file on the hard drive, or click **Browse** to redirect to another location

- **Reference Number** and **Authorization Code**: Type the Reference Number and Authorization Code that were displayed when the Security Officer was registered
- **Password** and **Confirm**: Type and confirm a password to protect the content of the security store

Click **OK** to complete the operation.

- 4 The desktop security store is created and the new Security Officer is logged into Entrust Authority Security Manager Administration.



## Exercise 5: Register and activate additional administrative users

In this exercise, additional administrative users will be registered and activated for use later in the course.

- 1 Still logged into Entrust Authority Security Manager Administration as a Security Officer, register the following administrative users. (If you have logged out of the application, double-click the **Security Manager Administration** icon on the desktop or click **Start > Apps > Entrust > Security Manager Administration**.) Place these users in the default group on the **General** Tab.
  - Two users with the Administrator role
  - One user with the Auditor role
  - One user with the Directory Administrator role
- 2 Create the digital ID for each administrative user using your preferred method. Keep track of the location of each security store as it will be needed to log in as that user.  
Record the names and roles of the user on your User planning worksheets.
- 3 Log into Entrust Authority Security Manager Administration as each newly-created administrative user and note the changes in the interface for each user role.



**Note:**

Multiple instances of Entrust Authority Security Manager Administration are allowed.

- 
- 4 When you are done, close all Entrust Authority Security Manager Administration windows.

## Managing Key Pairs

This lab has no exercises but there are discussion questions.

## Discussion Questions

- 1 Why do we retain a copy of the private decryption key of a 2 key pair user?
- 2 Where should the signing key pair be generated?
- 3 When is the policy viewed and why?

## Entrust Security Provider Lab

This module will introduce you to the main desktop client available for Entrust PKI. Security Provider deployment packages will be created and installed in the lab, then you will have a working client application to use for the remainder of the training.

## Lab

In these exercises, participants will build a customized installation of Entrust Entelligence Security Provider, which will then be installed on their computer allowing them to login to their digital ID as an end user. Cryptographic operation, such as encryption, will be tested.

## Tasks

The following tasks will be completed:

Exercise 1: Build an Entrust Entelligence Security Provider installation package

Exercise 2: Install Entrust Entelligence Security Provider

Exercise 3: Register new end users

Exercise 4: Activate a digital ID as an end user

Exercise 5: Log into the Entrust digital ID

Exercise 6: View Entrust Entelligence Security Provider options

Exercise 7: View certificate details using the Entrust Entelligence Security Provider Certificate Explorer

Exercise 8: Entrust Entelligence Security Provider Cryptographic Operations

Exercise 9: Encrypt a file for another user

Exercise 10: Decrypt a file

Exercise 11: Log out of the security store

Exercise 13: Securely delete a file

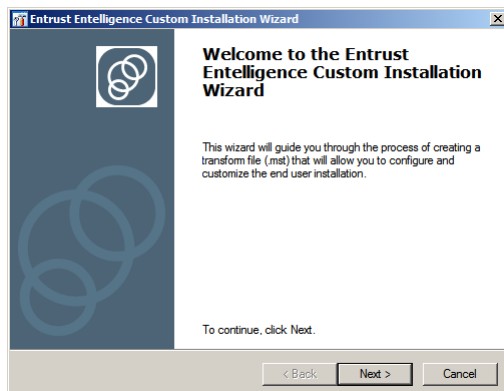
## Timing

Estimated time to complete these exercises is 90 minutes

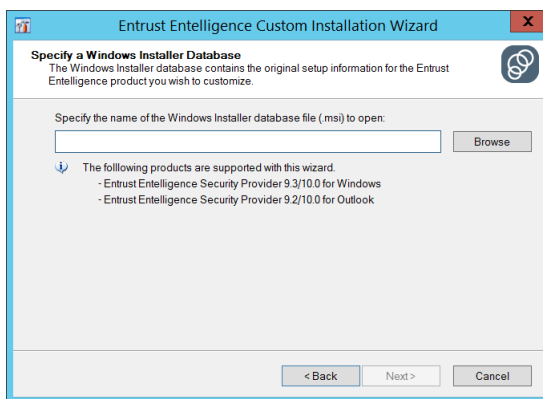
## Exercise 1: Build an Entrust Intelligence Security Provider installation package

In this exercise a customized installation package for Entrust Intelligence Security Provider will be created.

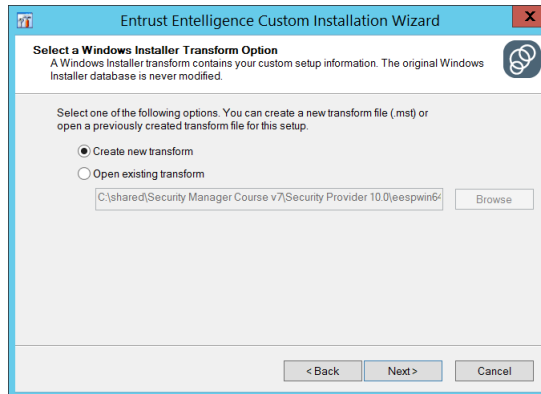
- 1 Locate and double-click the `eecustwiz.exe` file from the `...\Source\Security Provider 10` folder (or an alternate location indicated by the instructor). Click **Next** to begin the Wizard.



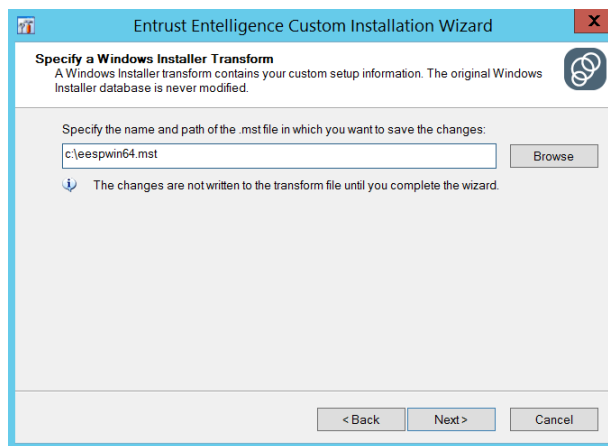
- 2 Click **Browse** to locate the `eespwin64.msi` file in the `C:\Source\Security Provider 10.0` folder (or an alternate location indicated by the instructor) and click **Open**. Click **Next** to continue.



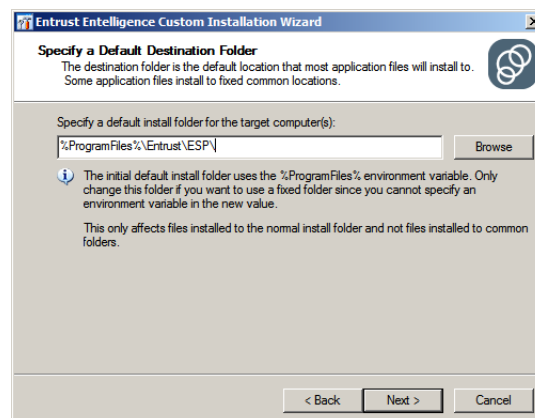
- 3 In the **Select a Windows Installer Transform Option** dialog box click **Create new transform**. The custom setting enabled in the wizard are stored in this new transform file. Click **Next** to continue.



- 4 Change the path to the `eespwin64.mst` file that will be created to `C:\eespwin64.mst`. Click **Next**.



- 5 The **Specify a Default Destination Folder** dialog box allows you to specify where the Entrust Intelligence Security Provider program files will be installed on the end user computers. Accept the default destination folder or type a new path and click **Next**.





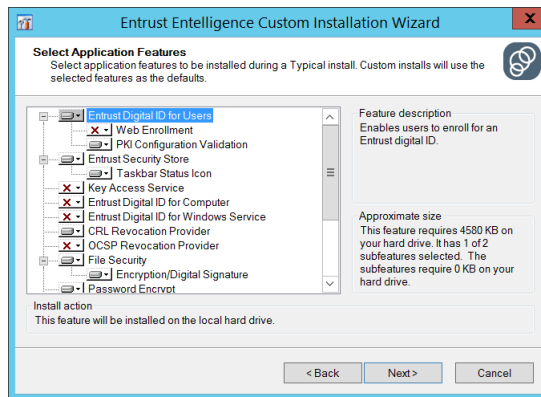
**Note:**

If this folder does not exist on the end user computer when the application is installed, the user will be prompted to accept the creation of the folder.

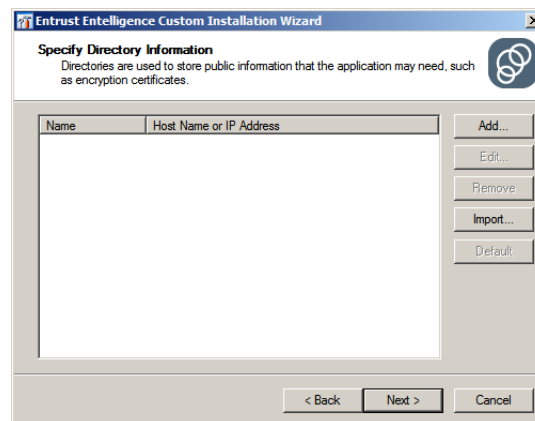
- 6 The **Select Applications Features** dialog box allows you to select the additional features required in the installation. Note that some mandatory components can not be deselected.

A hard drive icon indicates that the feature will be installed. A red X icon indicates that the feature will not be added to the installation. A description of each item is displayed in the **Feature Description** frame when a particular feature is clicked. Enable or disable features as needed.

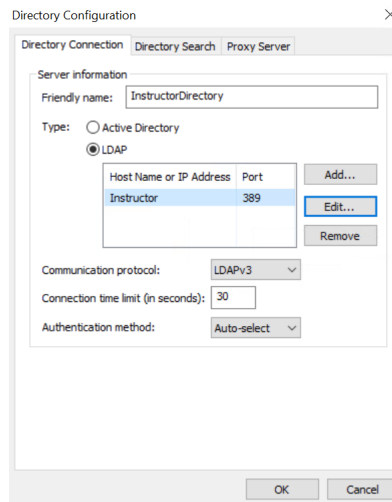
Enable **Entrust TrueDelete** in the list and click **Next**.



- 7 Select **Web Enrollment** to remove the X and install this feature.
- 8 The **Specify Directory Information** dialog box displays the Directory to be used by the client to retrieve public information.



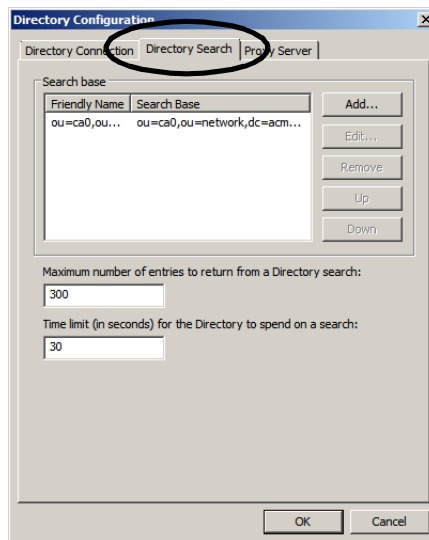
The Directory information is available in the `entrust.ini` file. Click **Import** and locate the `entrust.ini` file in the `C:\authdata\manager` folder. The Directory information from the `entrust.ini` file will be displayed.



Type a **Friendly Name** for the Directory to be displayed in the interface, for example, Instructor Directory.

In the Type: section, click the **Edit** button and change the Host IP to a Host name of Instructor.

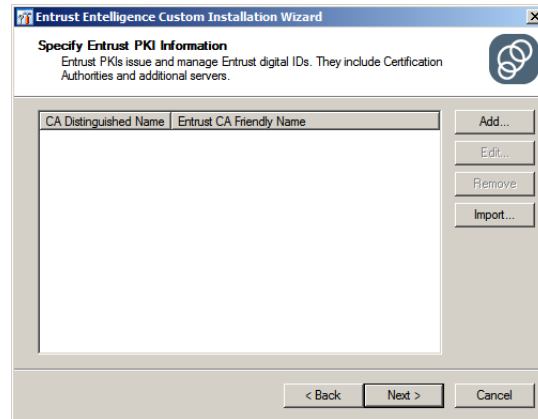
- 9 Click the **Directory Search** tab. This tab will list the searchbase that will be used to locate users.



- 10 Click Add and add in the searchbase to a partners CA so we can exchange certificates later in cross certification.i.e. `ou=ca1,ou=training,dc=entrust,dc=com`.

No Proxy Server is used in the classroom so this tab can be ignored. Click **OK** to accept the values entered. Click **Next** to continue.

- 11 The **Specify Entrust PKI Information** dialog box is displayed.



- Click **Import** and browse to locate the `entrust.ini` file in the `C:\authdata\manager` folder once again and click **Open**. If there is no `entrust.ini` available, click **Add** and type the required information in the appropriate fields of the dialog box.
- 12 Verify that the information on the following tabs is correct.

## Certification Authority

Entrust PKI Configuration ✕

|                         |                 |           |                |
|-------------------------|-----------------|-----------|----------------|
| Auto-Enrollment         | OCSP Responders | CardMS    | IdentityGuard  |
| Certification Authority | Policy          | Directory | Roaming Server |
| Proxy Server            |                 |           |                |

Server information

Host name or IP address:

Port number:

Distinguished name

DN:

Display information

Friendly name:

☒ Display this CA during enrollment and recovery

Display Order:

☐ Hide this CA during enrollment and recovery

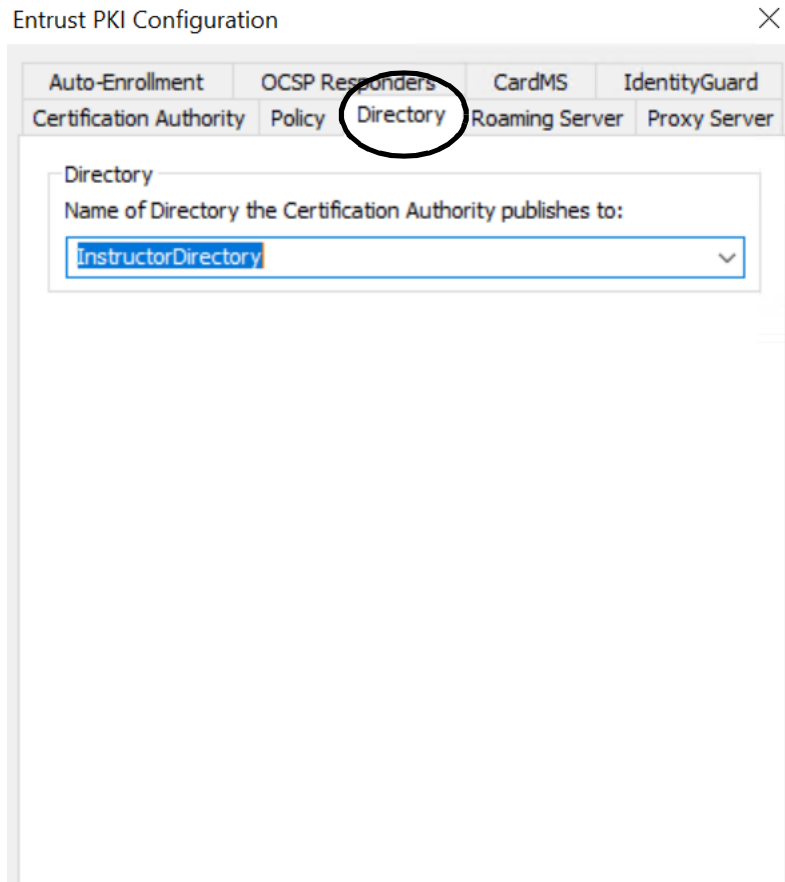
Entrust Authority Administration Services

Enrollment URL:

Recovery URL:

Click **Check Connection** and **Verify** to confirm that information has been entered correctly. Type a friendly name, for example, `InstructorCA` to identify your Certification Authority in the interface.

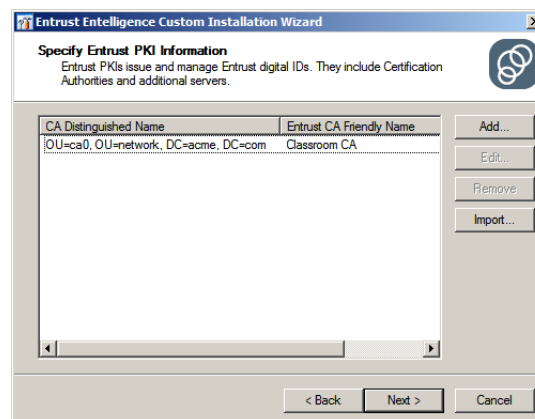
## Directory



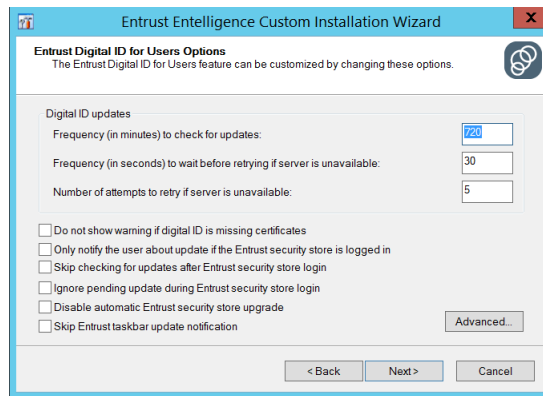
Select the Directory associated with the PKI by choosing it from the **Name of Directory Certificate Authority publishes to:** list. The names of the Directories displayed in this list are retrieved from the Directory information entered on the previous tab.

Click **OK** and **OK**.

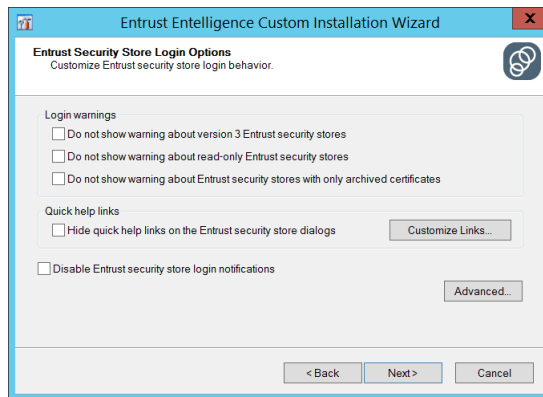
- 13 A list with the PKI entry will be presented. Click **Next**.



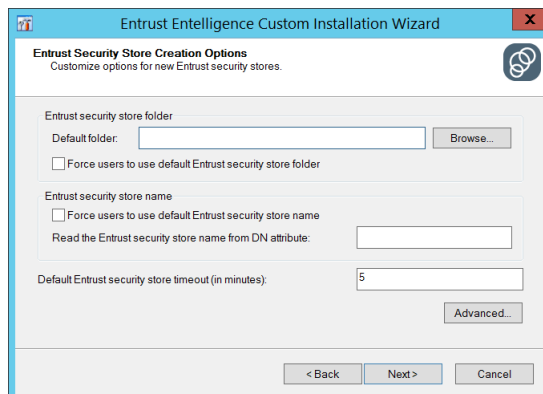
- 14 Accept the default values in the **Entrust Digital ID for Users Options** dialog box by clicking **Next**.



- 15 Accept the default settings in the **Entrust Security Store Login Options** dialog box by clicking **Next**.



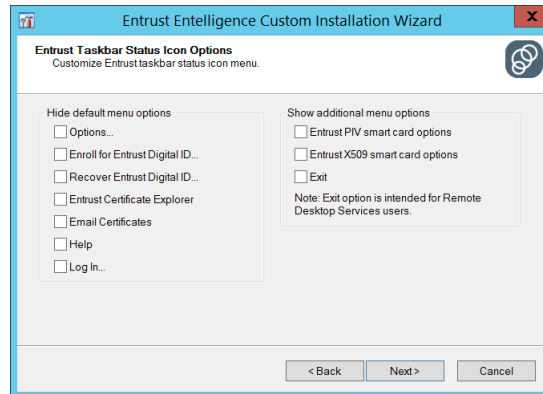
- 16 In the **Entrust Security Store Creation Options** dialog box modify the settings related to the location of the user security store.



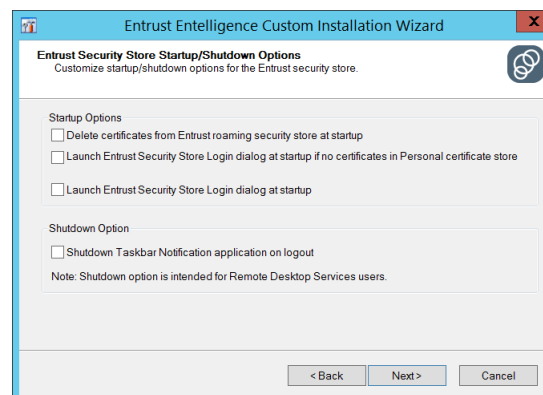
Type the path of a folder for storing Entrust desktop security stores, for example, `C:\authdata\manager\epf` and enable **Force users to use default Entrust security store folder**. This will force users to place their \*.epf files in this location.

Click **Next**.

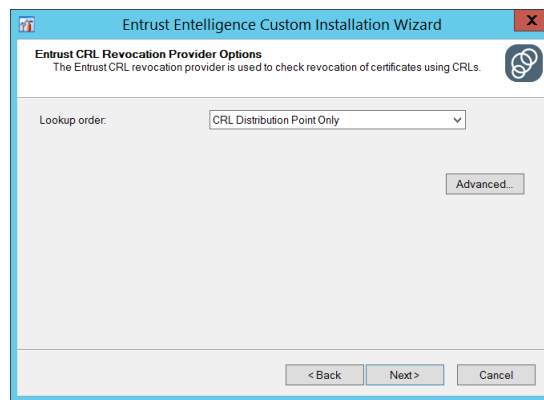
- 17 Accept the default values in the **Entrust Taskbar Status Icon Options** dialog box by clicking **Next**.



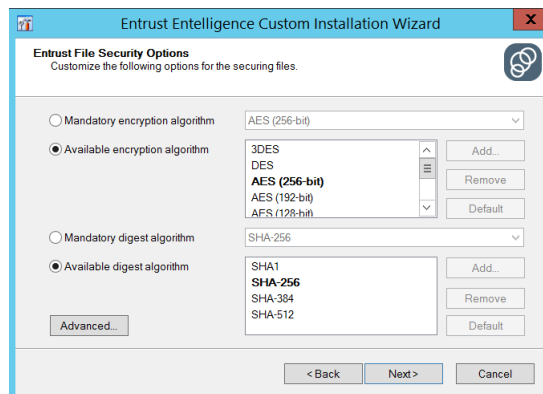
- 18 Accept the default values in the **Entrust Security Store Startup/Shutdown Options** dialog box by clicking **Next**.



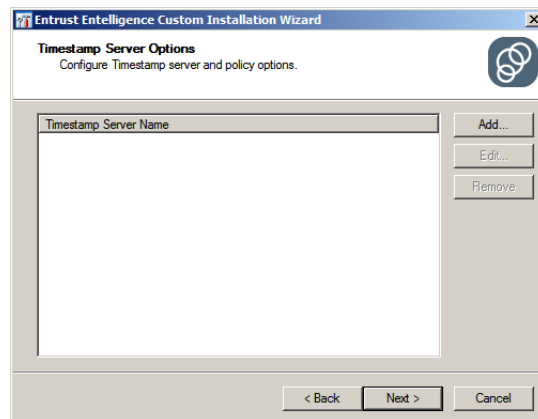
- 19 Select **CRL Distribution Point only** in the **CRL Revocation Provider Options** dialog box and click **Next**. This option disables the caching of revocation information on the client computer.



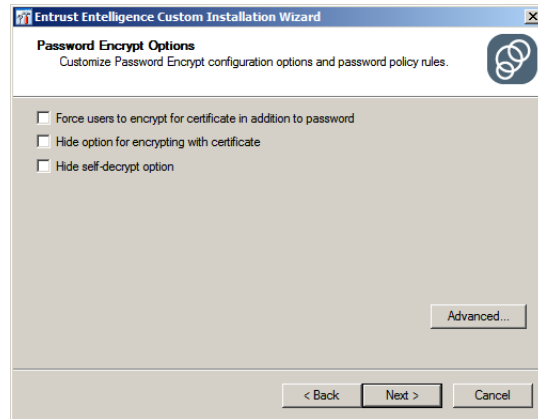
- 20 Accept the default settings in the **Entrust File Security Options** dialog by clicking **Next**.



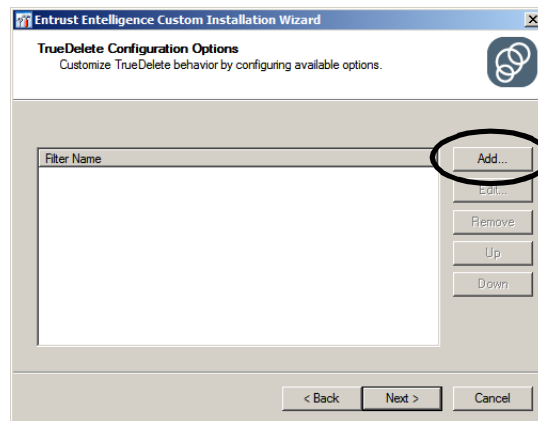
- 21 No Timestamp Server is installed in the infrastructure, click to **Next** to continue.



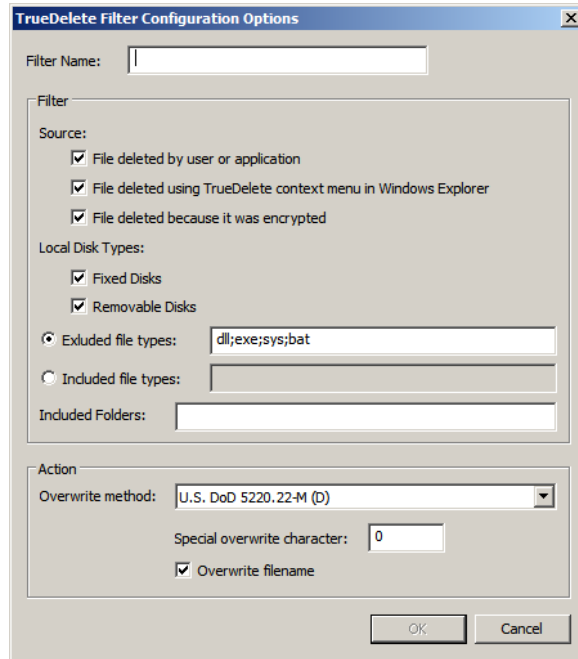
- 22 Accept the default settings in the **Password Encrypt Options** dialog by clicking **Next**.



- 23 Entrust TrueDelete was enabled when the installable components of Entrust Intelligence Security Provider were defined. The details of the TrueDelete filter must be defined.



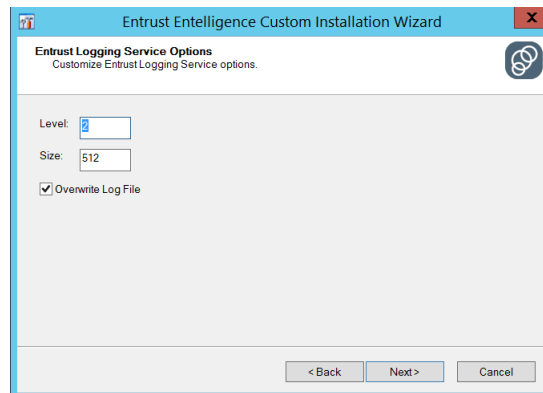
Click **Add** to create a filter.



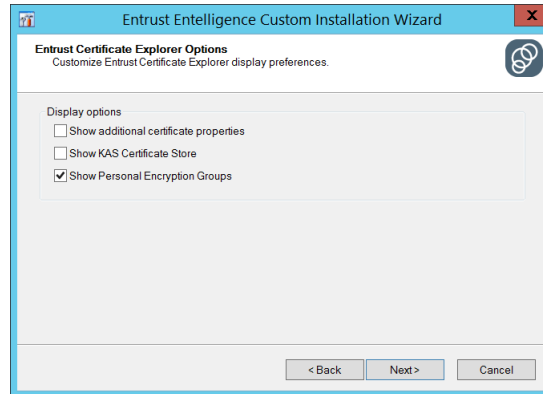
- **Filter Name:** Type a name for the filter, for example, Classroom Delete
- **File deleted by user or application:** Enable
- **Overwrite method:** Select a delete standard to be used by TrueDelete
- Create a second filter with a different Overwrite method selected so you have two to choose from

Click **OK** and **Next**.

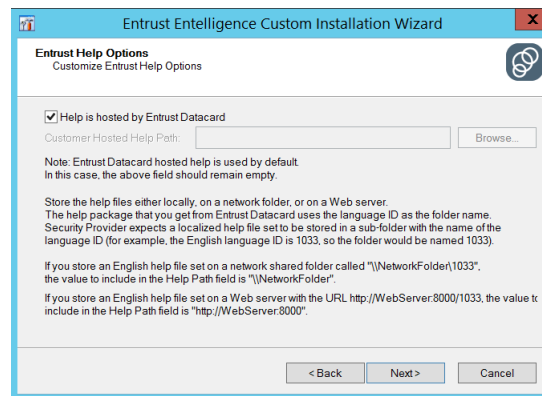
24 Accept the default settings in the **Entrust Logging Service Options** dialog by clicking **Next**.



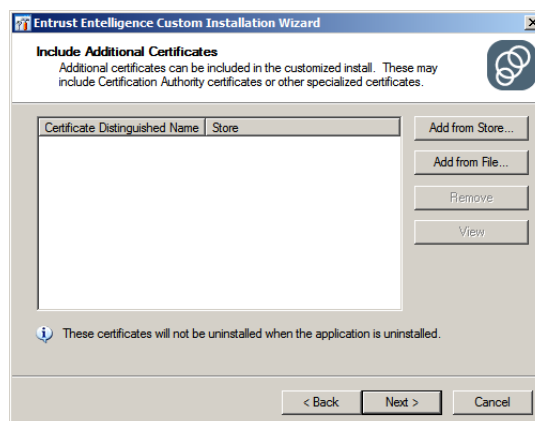
- 25 Accept the default settings in the **Entrust Certificate Explorer Options** dialog by clicking **Next**.



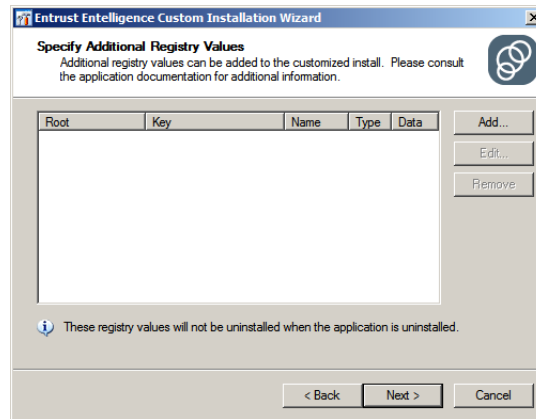
- 26 Accept the default settings in the **Entrust Help Options** dialog by clicking **Next**.



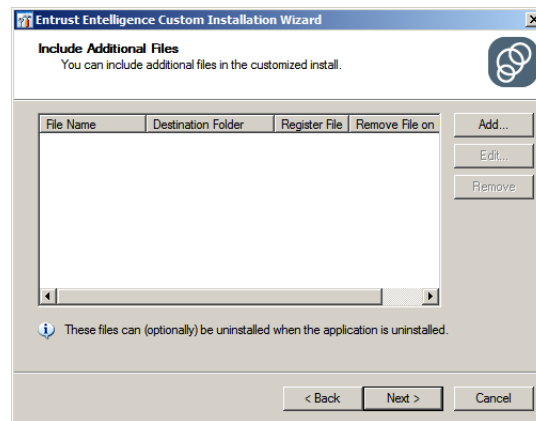
- 27 No additional Certification Authority certificates are to be distributed to the end user computers. Click **Next**.



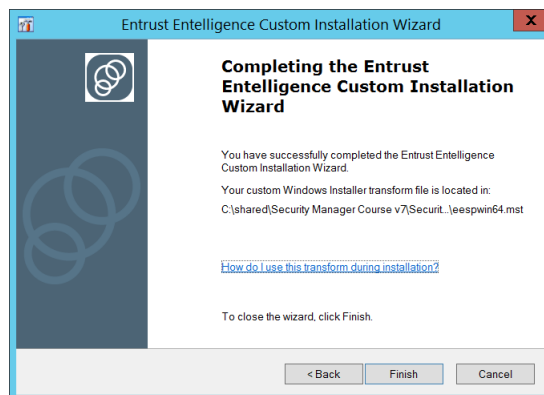
- 28 No additional values are be added to the Windows registry on the end user computer. Click **Next**.



- 29 No additional files are be added to the end user computer. Click **Next**.



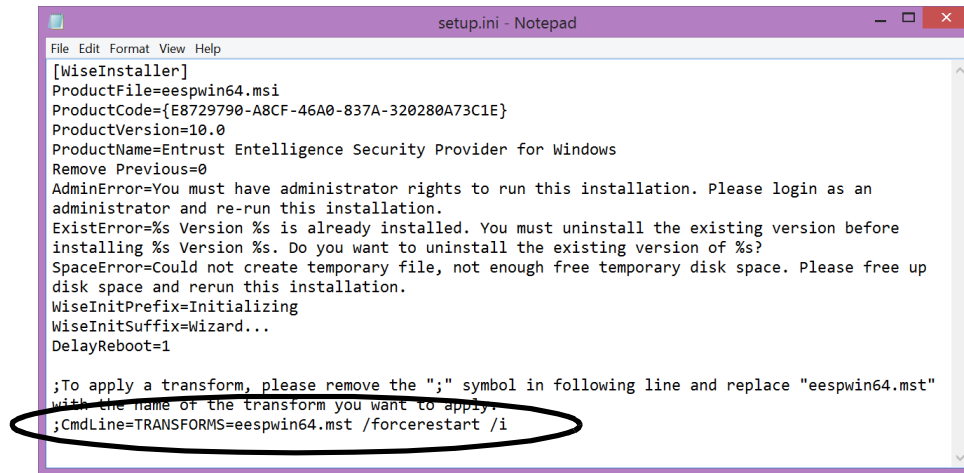
- 30 Click **Finish** to complete the configuration wizard.



The \*.mst file is created in the specified folder.

- 31 Copy the following files from ... \Source \Security Provider 10 to the same folder as the eespwin64.mst (for example, C:\):
- eespwin64.msi

- license.txt
  - setup.exe
  - setup.ini
- 32 Open the `setup.ini` file and apply the transform file by **removing the ; (semi-colon)** from the `CmdLine=` entry. If the name of the \*.mst file was changed during configuration, make sure to update the entry to reflect the correct name for the transform file.
- Save the `setup.ini` file.



```
[WiseInstaller]
ProductFile=eespwin64.msi
ProductCode={E8729790-A8CF-46A0-837A-320280A73C1E}
ProductVersion=10.0
ProductName=Entrust Entelligence Security Provider for Windows
Remove Previous=0
AdminError=You must have administrator rights to run this installation. Please login as an
administrator and re-run this installation.
ExistError=%s Version %s is already installed. You must uninstall the existing version before
installing %s Version %s. Do you want to uninstall the existing version of %s?
SpaceError=Could not create temporary file, not enough free temporary disk space. Please free up
disk space and rerun this installation.
WiseInitPrefix=Initializing
WiseInitSuffix=Wizard...
DelayReboot=1

;To apply a transform, please remove the ";" symbol in following line and replace "eespwin64.mst"
;with the name of the transform you want to apply.
;CmdLine=TRANSFORMS=eespwin64.mst /forcerestart /i
```

The customized installation package is now created and is ready to be installed by the end users in your organization.

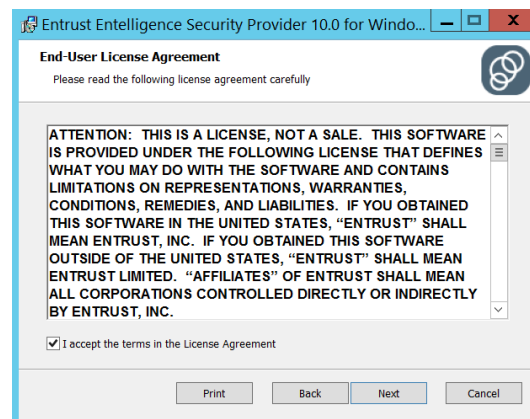
## Exercise 2: Install Entrust Intelligence Security Provider

In this exercise, you will install the customized Entrust Intelligence Security Provider package.

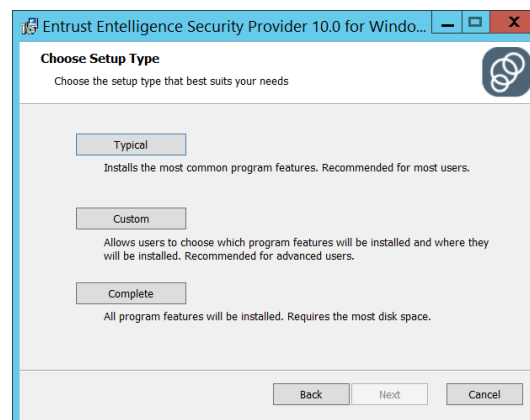
- 1 Locate and double-click the `C:\setup.exe` file.
- 2 A **Welcome** dialog box is displayed. Click **Next** to begin the installation.



- 3 If the terms of the license agreement are acceptable, click **I accept the terms in the License Agreement** and click **Next**.



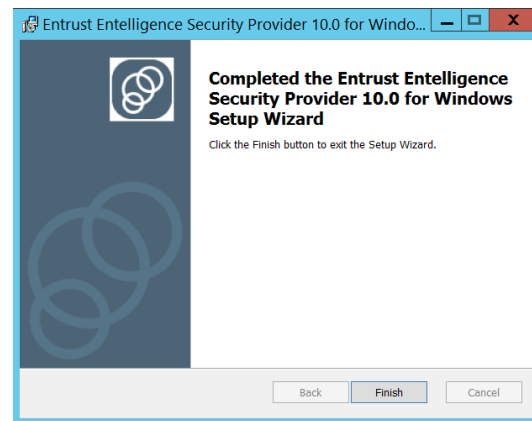
- 4 Click **Typical** installation.



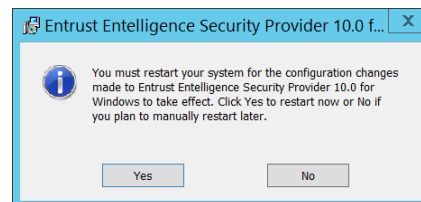
- Click **Install** to begin the installation of Entrust Entelligence Security Provider. The customization options describes in the \*.mst file will be applied to the \*.msi file to install the components.



- Click **Finish** to close the setup wizard.



- Click **Yes** to restart.



**Note:**

Remember to use the Security Manager Control Command Shell to start the Security Manager service after the machine reboot.

- 8 The Entrust Entelligence Security Provider icon is now displayed in the system tray at the lower-right-hand corner of the Windows screen.

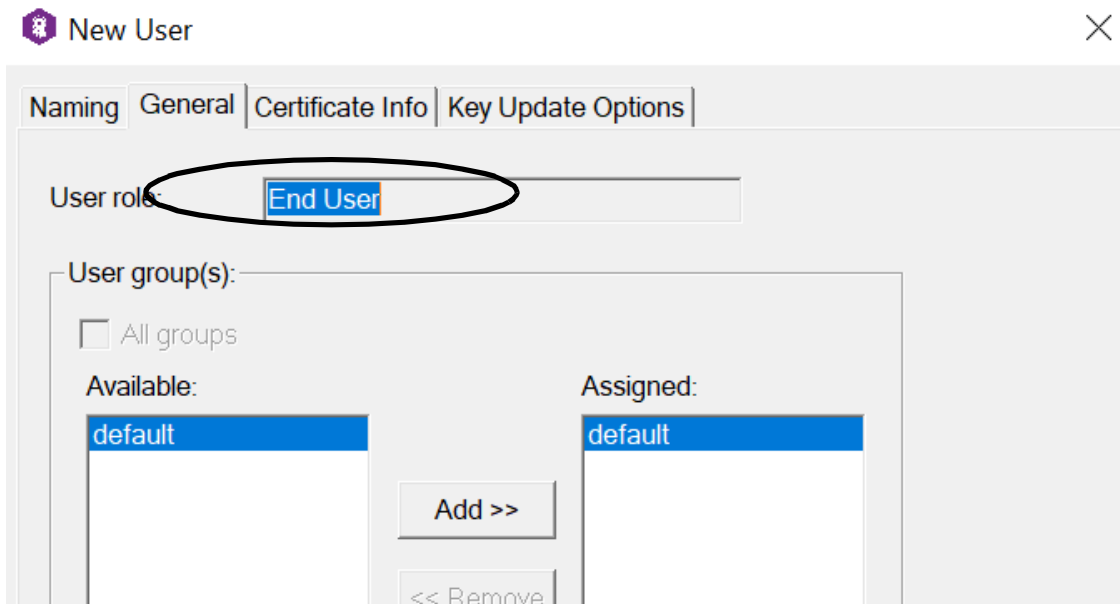


### Exercise 3: Register new end users

All users participating in the public-key infrastructure must be registered in Entrust Authority Security Manager. Registering an end user is the responsibility of an administrative user with appropriate permissions to perform this task.

In this exercise a user with the default **End User** role will be created. This user will activate their digital ID using Entrust Security Provider in the next exercise.

- 1 Log in to Entrust Authority Security Manager Administration as an **Administrator**.
- 2 Right-click **Users** and click **New User**.
- 3 Enter the necessary information is to register the end user:
  - **Naming:** Enter the **First Name** and **Last Name** for the user. A unique **Serial number** and an **Email** address can also be entered if required
  - **General tab:** Ensure that the **User role** is set to **End User**



**New User**

Naming | General | Certificate Info | Key Update Options

User role: **End User**

User group(s):

☐ All groups

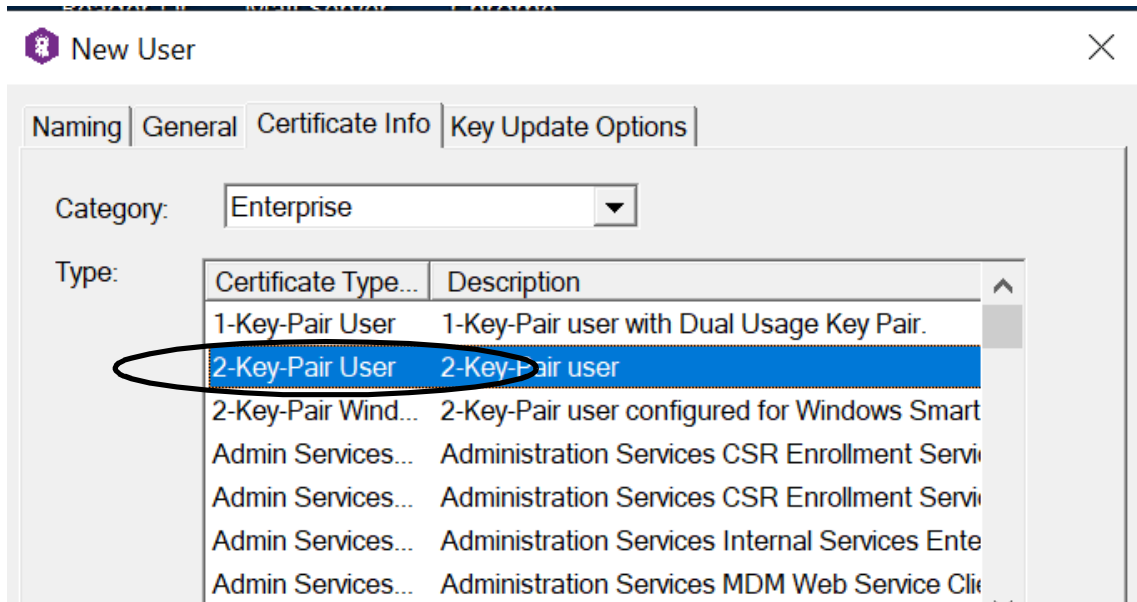
Available: default

Assigned: default

Add >>

<< Remove

- **Certificate Info:** Select the certificate **Category** of **Enterprise** and the certificate **Type** of **2-key-pair user**



- **Key Update Options:** Accept the default key update options
- When you have completed the required fields on all the tabs, click **OK**.

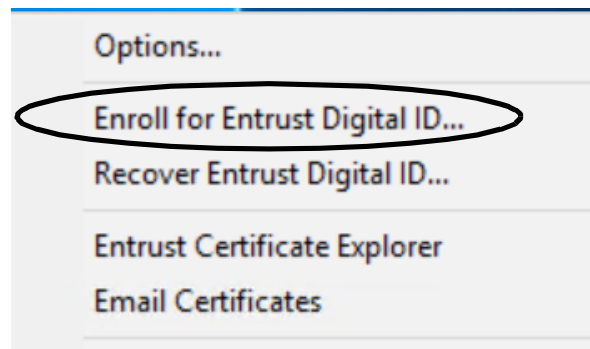
- 4 The **Reference number** and **Authorization code** are displayed.  
Record these activation codes.

Note that the new user is listed in the right-hand frame of the Entrust Authority Security Manager Administration window with the state of **Added**. You can view the properties for the end user, including the Reference Number and Authorization Code, by double-clicking the user's entry.

## Exercise 4: Activate a digital ID as an end user

Entrust Intelligence Security Provider is installed and the user has been registered in Entrust Authority Security Manager Administration. In the next exercise, the user will be activated through Entrust Intelligence Security Provider to create their Entrust digital ID.

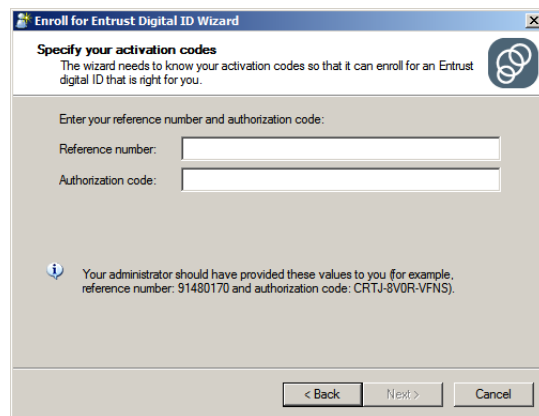
- 1 Click **Start > Apps > Entrust Intelligence > Enroll for Entrust Digital ID** or right-mouse-click on the Entrust Intelligence Security Provider icon in the system tray and click **Enroll for Entrust Digital ID**.



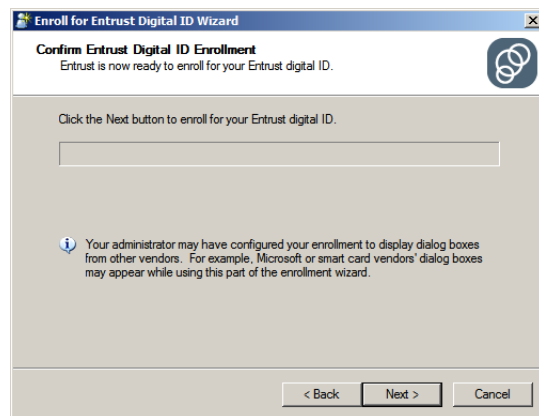
A **Welcome** dialog box is presented. Click **Next**.



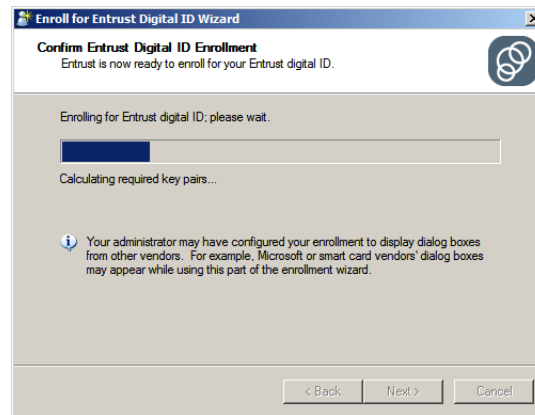
- 2 Type the **Reference Number** and **Authorization Code** for the registered user and click **Next**.



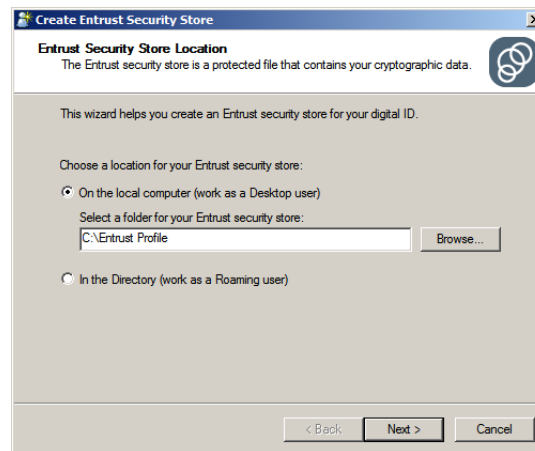
- 3 In the **Confirm Entrust Digital ID Enrollment** dialog box, click **Next** to begin the creation of the digital ID.



- 4 Policy certificates are retrieved from the Directory and the keys pairs are generated.



- 5 The **Entrust Security Store Location** dialog box is presented. If a location was enforced when the Entrust Intelligence Security Provider installation package was created, the user will be bound by that setting. If no location was indicated, click **Browse** and choose a location for the security store. Click **OK** and **Next**.



- 6 If the folder does not exist, you will be asked to create it. Click **Yes** to create the folder.



- 7 In the **Entrust Security Store Name** dialog box type the name for the security store. Typically, this field will be already filled in with the name of the user that is currently logged into Windows.

If not filled in correctly (as in the case in the classroom since you are logged into the computer as Administrator) type an appropriate name for profile and click **Next**.

The screenshot shows the 'Create Entrust Security Store' dialog box, specifically the 'Entrust Security Store Name' step. The title bar reads 'Create Entrust Security Store'. Below the title, the text 'Entrust Security Store Name' is followed by 'A name uniquely identifies your Entrust security store.' There is a text input field labeled 'Name:'. Below the field, a message states: 'Your Entrust security store name must not contain the following characters: \\/:\*?<>['. A green checkmark is visible to the left of this message. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

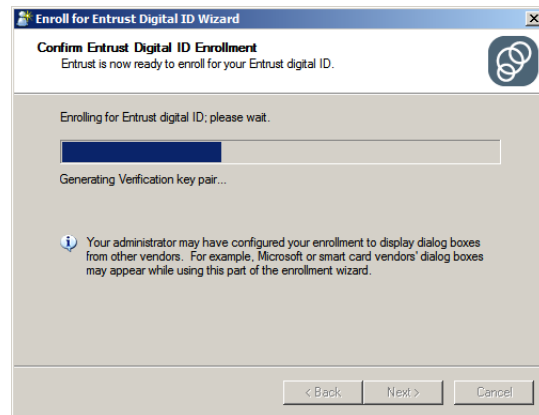
- 8 Type and confirm a password that will satisfy the rules listed. (In the classroom use the password of EntPKI2000.)

The screenshot shows the 'Create Entrust Security Store' dialog box, specifically the 'Entrust Security Store Password' step. The title bar reads 'Create Entrust Security Store'. Below the title, the text 'Entrust Security Store Password' is followed by 'Password rules help ensure you select a secure password to protect your Entrust security store.' There are two text input fields: 'Password:' and 'Confirm Password:'. Below the fields, a message states: 'Your password must satisfy the following rules:'. A list of five rules follows, each preceded by a red 'X' icon: 'must be at least 8 characters long', 'must contain an uppercase character', 'must contain a lowercase character', 'must not contain a portion of security store name longer than half its length', and 'must not repeat a character more than half the length of password'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

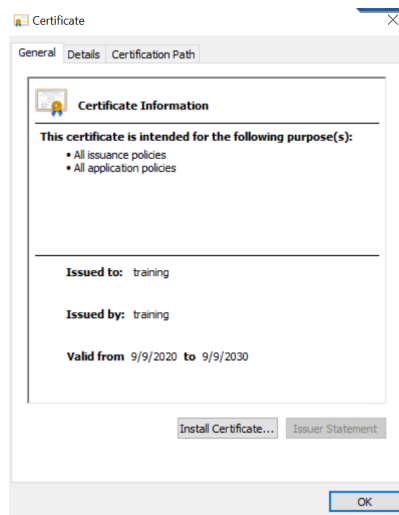
As the password is typed a green check mark is displayed next to each rule as they are satisfied. Click **Finish**.

The screenshot shows the 'Create Entrust Security Store' dialog box, specifically the 'Entrust Security Store Password' step. The title bar reads 'Create Entrust Security Store'. Below the title, the text 'Entrust Security Store Password' is followed by 'Password rules help ensure you select a secure password to protect your Entrust security store.' There are two text input fields: 'Password:' and 'Confirm Password:', both filled with dots. Below the fields, a message states: 'Your password must satisfy the following rules:'. A list of five rules follows, each preceded by a green checkmark icon: 'must be at least 8 characters long', 'must contain an uppercase character', 'must contain a lowercase character', 'must not contain a portion of security store name longer than half its length', and 'must not repeat a character more than half the length of password'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

9 The security store is created.



10 If the verification certificate of your Certification Authority is not already in the Windows certificate store, a **Security Warning** message appears. Click **Yes** to install the certificate.



11 Click **Finish** to close the wizard.

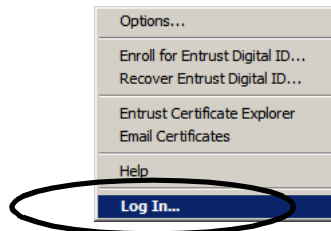


The end user security store, in this case a desktop profile, has been created.

## Exercise 5: Log into the Entrust digital ID

The password provided on the Entrust login screen is used to decrypt the keys and certificates in the security store. Logging in to the security store is not usually required proactively. In most cases, the user will be prompted to log in when an application requires a private key protected in the security store. In this exercise, you will manually log in to the digital ID.

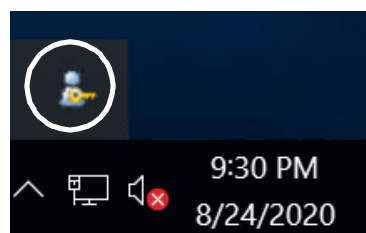
- 1 Right-click the Entrust Intelligence Security Provider icon in the Windows system tray in the lower right hand corner of the screen and click **Log in**.



- 2 Click **Browse** to locate the desktop security store (the \*.epf file) you just created on the hard drive. Type the password assigned to the security store and click **OK**.



The Entrust Intelligence Security Provider icon in the system tray will change to indicate that the user is logged into their digital ID.



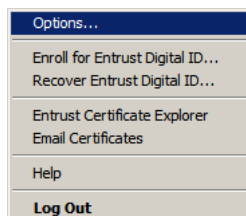
### Note:

If the user security store is on a smartcard or token, the Entrust login dialog box will never be displayed. Instead, the vendor of the smartcard or token will be responsible for the login process. In this scenario, logging into the smartcard or token by typing a password will be handled by the smartcard or token vendor's software.

## Exercise 6: View Entrust Intelligence Security Provider options

In this exercise, you will view application options for a logged-in user.

- 1 Right-click the Entrust Intelligence Security Provider icon in the system tray and click **Options**.



The **Entrust Security Store Options** dialog box is displayed.



From this window the end user can change their log out timing and logout hot key shortcut. If roaming is enabled and the appropriate policy settings are selected, users can switch from working as a desktop user to a roaming user and back at will.

Some options, such as the ability to change a password and assign a timeout are available to users of a desktop security store only.

- 2 Click **Change Password** to launch the **Entrust Security Store Password Wizard** to step the user through this process. Click **Cancel** to close the Wizard.

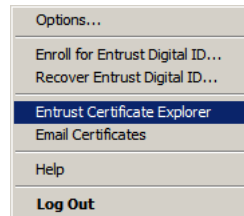


- 3 Click **OK** to close the **Entrust Security Store Options** dialog box.

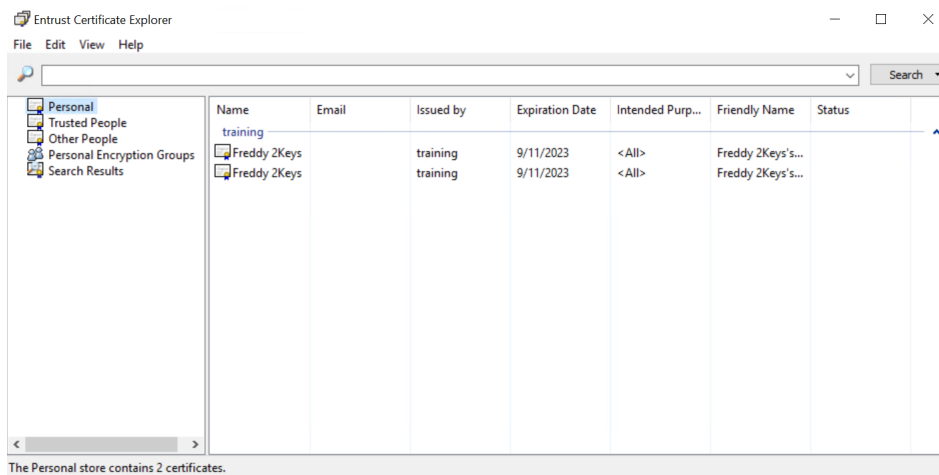
## Exercise 7: View certificate details using the Entrust Intelligence Security Provider Certificate Explorer

In this exercise, participants will use Entrust Intelligence Security Provider Certificate Explorer to view certificates on their computer.

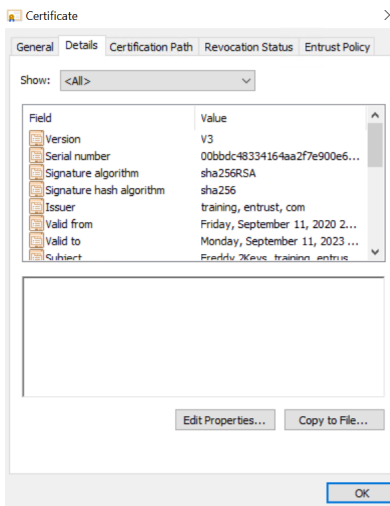
- 1 Right-click the Entrust Intelligence Security Provider icon in the system tray. Click **Entrust Certificate Explorer**.



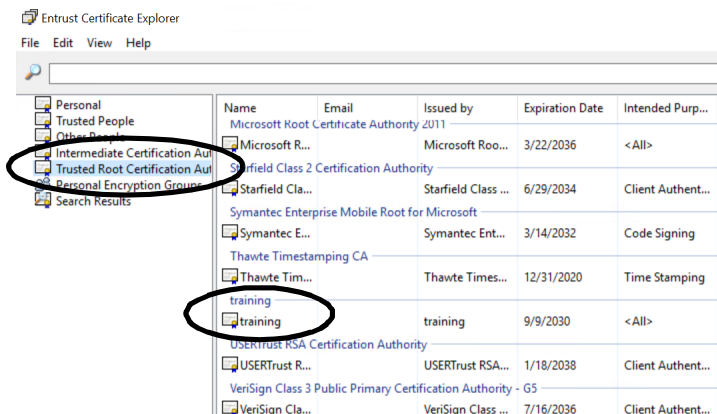
The **Entrust Certificate Explorer** window is displayed.



- 2 Double-click a certificate in the list and click the **Details** tab. Scroll to view the fields and extensions



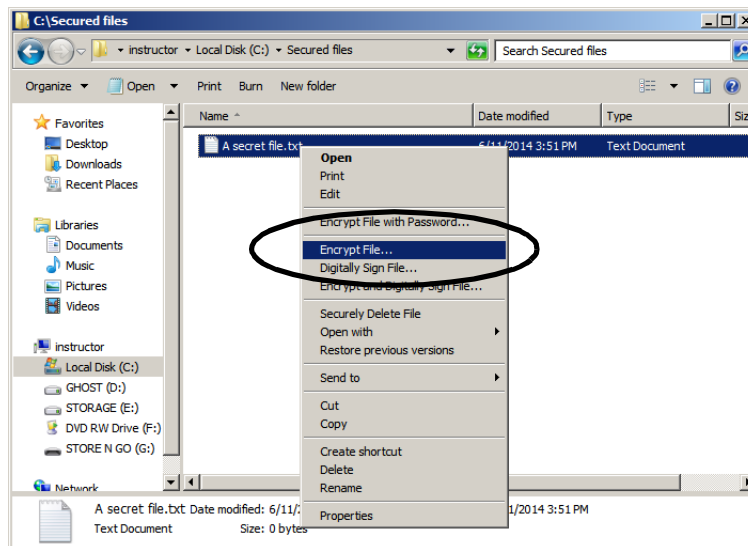
- 3 Click **OK** to close the certificate viewer.
- 4 Click **View > CA Certificates** to view the verification certificates of Certification Authorities that are stored in the Windows certificate store on your computer.
- 5 Click **Trusted Root Certification Authorities** in the left-hand pane. The verification certificates are displayed, you should see the verification certificate for your own Certification Authority displayed.



## Exercise 8: Entrust Intelligence Security Provider Cryptographic Operations

In this exercise, Entrust Intelligence Security Provider's cryptographic components will be used to encrypt and decrypt files.

- 1 Create a text file and type some information in the file. Save the file to the hard drive on your computer.
- 2 Locate and right-click the file in Windows Explorer. The Entrust Intelligence Security Provider cryptographic options are displayed on the context-sensitive menu. Click **Encrypt File**.

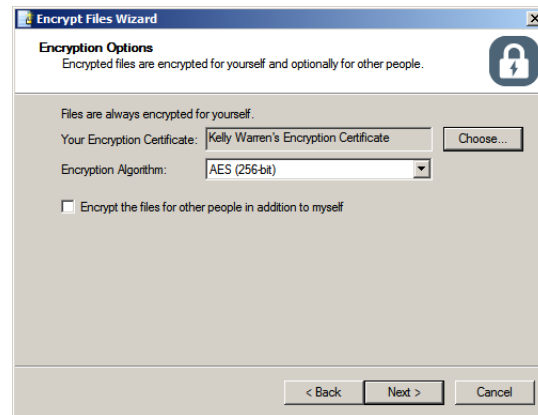


- 3 The **Encrypt Files Wizard** is displayed. Click **Next**.



- 4 The encryption certificate for the user who was last logged into Entrust Intelligence Security Provider is displayed. The file can be encrypted for that user or click **Choose** to select a different

certificate from the Windows store. The symmetric algorithm used to encrypt the data can also be selected, depending on the policy settings for the user. Click **Next**.



- 5 The file is encrypted. You can choose to have the plain text version automatically deleted. Click **Finish**. A file with a \*.p7m extension is created; this is the encrypted version of the file.

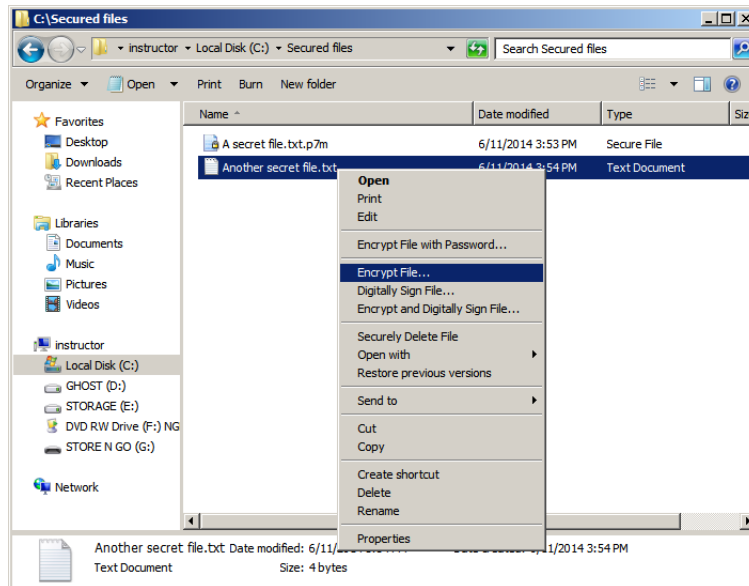


## Exercise 9: Encrypt a file for another user

In this exercise, you will encrypt a file for another user in your Entrust Authority Security Manager domain.

- 1 Create a second text file and type some information in the file. Save the file to the hard drive on your computer.

- 2 Right-click on the file and click **Encrypt File**.



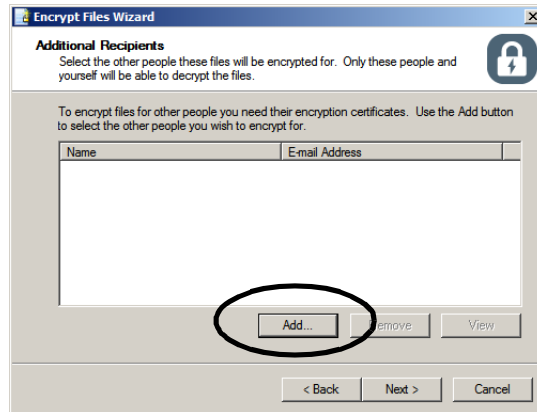
- 3 The **Encrypt Files Wizard** is presented. Click **Next**.



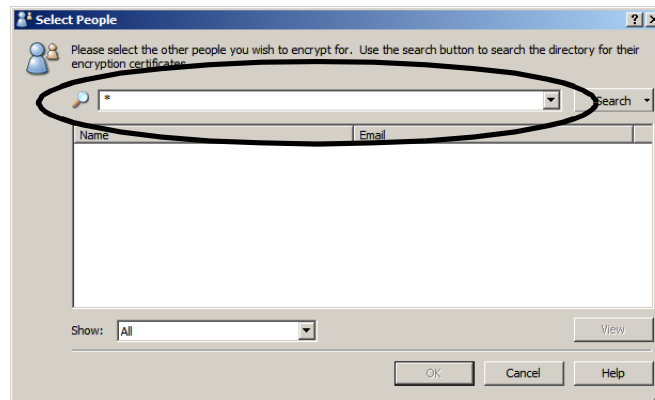
- 4 Click **Encrypt the files for other people in addition to myself** and click **Next**.



- 5 The **Additional Recipients** dialog box is displayed. Click **Add**.



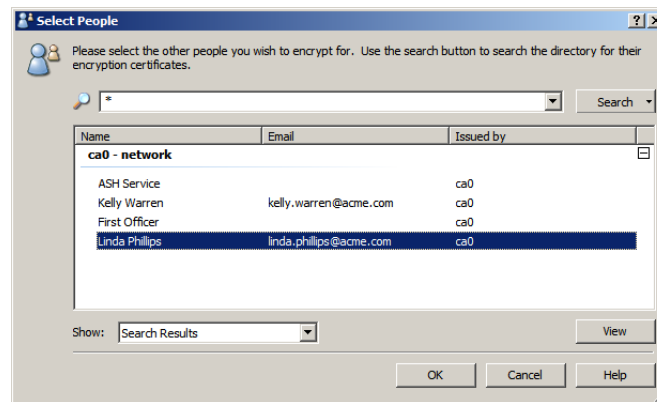
- 6 The **Select People** dialog box will allow you to search the Directory for the encryption certificates of other users. To search for certificates in all allowable searchbases in the Directory, type \* (the wildcard character to search for all users) and click **Search**.



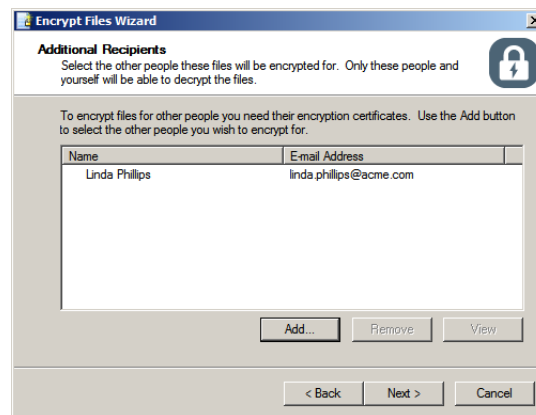
**Note:**

Entrust Entelligence Security Provider uses the searchbases entered during the creation of the customized installation package, not the searchbases indicated in Entrust Authority Security Manager Administration.

- 7 Click (or multi-click by holding down the <Ctrl> key) to select the recipient(s) of the encrypted file and click **OK**.



- 8 Click **Next** to confirm the choices in the **Additional Recipients** dialog box.



- 9 Click **Finish** to close the **Encrypt Files Wizard**.

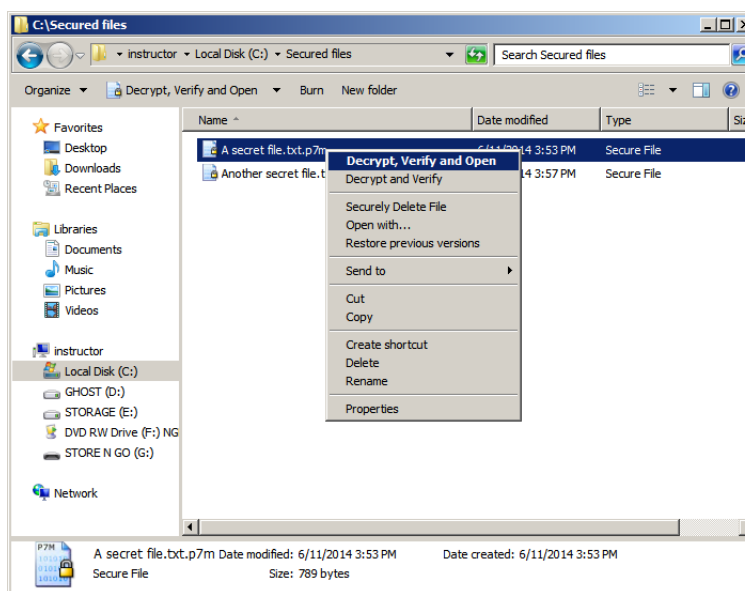


- 10 Ensure that **no users** are currently logged into **Entrust Entelligence Security Provider**.

## Exercise 10: Decrypt a file

In this exercise, the encrypted files will be decrypted by their intended recipients.

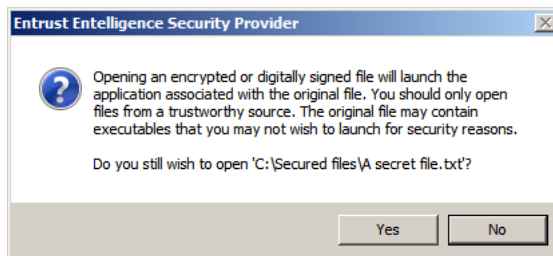
- 1 Right-click the first file that was encrypted (note the .p7m extension) and select **Decrypt, Verify and Open**.



- 2 The **Entrust Security Store Login** dialog box appears. Login by locating the desktop security store file and typing the password for the user and click **OK**.

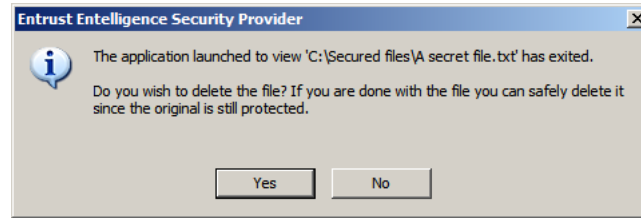


- 3 Click **Yes** to decrypt and open the file.



- 4 The file is decrypted and opened.

- 5 Close the text file and when prompted, click **No** to delete the plain text file.

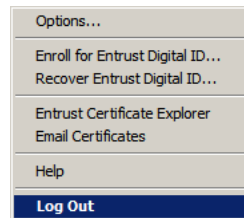


- 6 Log out of the security store.
- 7 Decrypt and open the second encrypted file.
- 8 Delete the **encrypted** version of both files. There should now be only two plain text files.

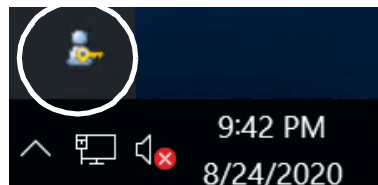
## Exercise 11: Log out of the security store

When a user is logged into the security store, it is very important that they log out when stepping away from their computer. This will prevent another user from coming to their computer and signing a message or decrypting a file while impersonating the user. The end user will be logged out automatically based on the timeout setting in Options and in the user policy. In this exercise, the user will manually log out of the security store.

- 1 With an end user still logged into their security store, right-click the Entrust Entelligence Security Provider icon in the system tray and click **Log Out**.



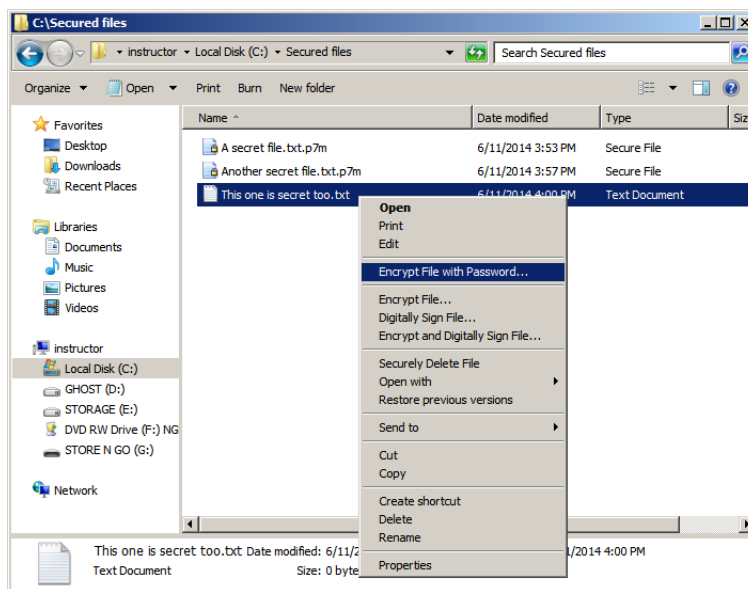
- 2 The icon will change to indicate that the user is logged out.



## Exercise 12: Password encrypt a file

In this exercise, one of the text files will be encrypted with a password instead of an encryption certificate. This will allow you to send secured information to users outside your Certification Authority trust domain. You would only need to communicate the password to the recipient of the file.

- 1 Right-click on one of your text files and click **Encrypt Files with Password**.



- 2 The **Password Encrypt Files Wizard** is presented. Click **Next**.



- 3 Click to deselect **Encrypt the files for my encryption certificate in addition to the password**. Type and confirm a password for the file. The policy rules for the password used to encrypt the file are display as red Xs that change to green check marks as the rules are satisfied. Click **Next**.

The screenshot shows the 'Password Encrypt Files Wizard' dialog box, specifically the 'Encryption Options' tab. The title bar reads 'Password Encrypt Files Wizard'. Below the title bar, the tab is labeled 'Encryption Options' with a subtitle: 'Encrypted files are encrypted for a password and optionally for your encryption certificate.' A lock icon is visible in the top right corner. The main area contains the text: 'Files are always encrypted with the password you specify.' Below this are two text input fields labeled 'Password:' and 'Confirm Password:'. A list of password rules is shown, each preceded by a red 'X' icon: 'must be at least 8 characters long', 'must contain an uppercase character', 'must contain a lowercase character', and 'must contain a numeric character'. At the bottom, there is a checkbox labeled 'Encrypt the files for my encryption certificate in addition to the password', which is currently unchecked. Below the checkbox is a text field labeled 'Your Encryption Certificate:' containing the text 'Kelly Warren's Encryption Certificate', and a 'Choose...' button. At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 4 Click **Generate self-decrypting output file** and click **Next**.

The screenshot shows the 'Password Encrypt Files Wizard' dialog box, specifically the 'Packaging Options' tab. The title bar reads 'Password Encrypt Files Wizard'. Below the title bar, the tab is labeled 'Packaging Options' with a subtitle: 'Multiple files may be combined into a single encrypted output file and optionally into a self decrypting executable.' A lock icon is visible in the top right corner. The main area contains a checkbox labeled 'Combine all files into single output file', which is checked. Below this is a text input field containing the path 'C:\Secured files\This one is secret too.txt.exe' and a 'Browse' button. Below the text field is another checkbox labeled 'Generate self-decrypting output file', which is also checked. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

When **Generate self-decrypting output file** is enabled, the file is encrypted and is embedded it within an \*.exe file. The \*.exe file can be distributed, along with the password, to your recipients. They do not require any special software.



**Note:**

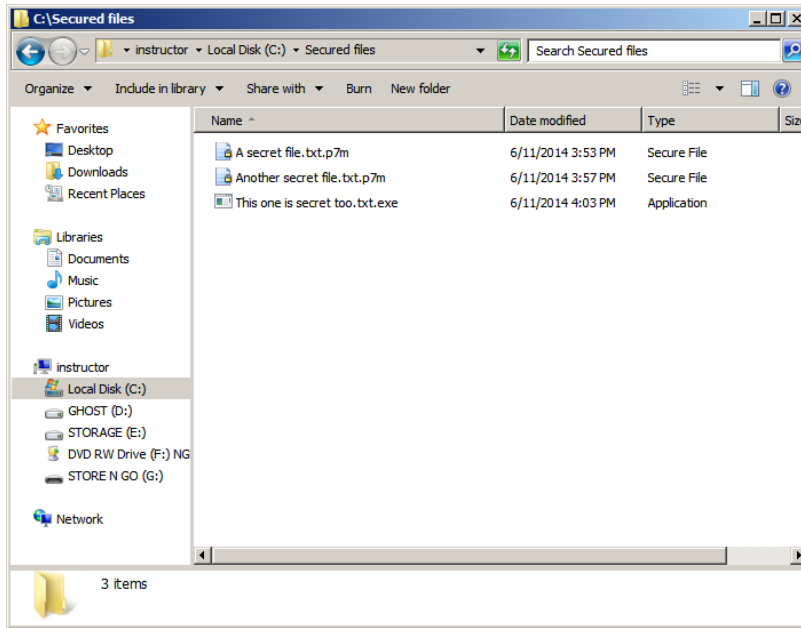
Be mindful when emailing self-decrypting output files to your recipients as many popular email applications will filter out executable files from e-mail messages. An alternate method is to disable the creation of a self-decrypting output file and have your recipient download a free decryption tool from the Entrust Web site.

---

- 5 The **Completing the Password Encrypt Files Wizard** dialog box is presented. Click **Delete the original files on finish** to delete the plain text copies of these files. If email access was configured in Entrust Entelligence Security Provider, the file could be emailed directly at this point. Click **Finish**.



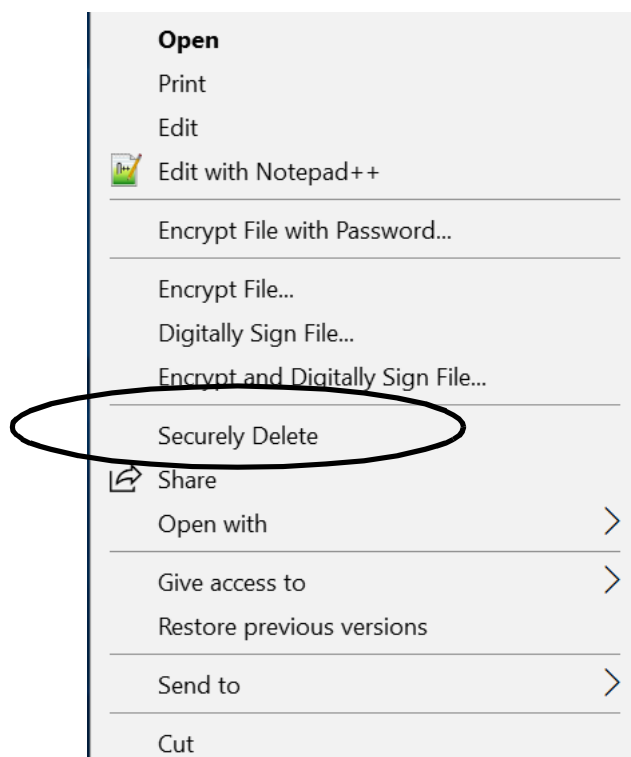
- 6 The \*.exe file is created and store on the hard drive in the chosen location.



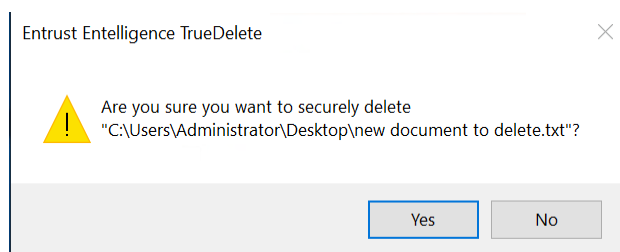
## Exercise 13: Securely delete a file

In this exercise, participants will permanently delete a file using Entrust TrueDelete. This component is optional in the Entrust Entelligence Security Provider installation, and was enabled during the creation of the customized installation.

- 1 On the desktop create a new file with notepad.
- 2 Close and save.
- 3 Right click on the file and select Securely Delete.



- 4 A confirmation message appears. If more than one delete profile was created with the wizard the options would be presented.



- 5 The file is removed completely, verify in the recycle bin.



## Managing users

This lab will test your administration skills with use case scenarios. Now that you have learned about the different ways to manage users, apply your skills here. Don't forget to not only consider the actions to perform but the underlying policies or decisions that may need to be made for each scenario.

## Lab

In these exercises, participants will perform user lifecycle management tasks on a collection of users. Scenarios are presented and course participants will need to decide which operation to use and perform the necessary steps.

### Tasks

The following tasks will be completed:

Exercise 1: User Lifecycle tasks

### Timing

Estimated time to complete these exercises is 45 minutes

## Exercise 1: User Lifecycle tasks

In your role as an administrative user, consider the scenarios listed in each step. Complete the following tasks using the appropriate administrative function in Entrust Authority Security Manager Administration.

Keep in mind that some operations might require you to log into Entrust Authority Security Manager Administration as a Security Officer and others are performed by administrative users, such as an Administrator. Use the Security Officer role only for operations that the Administrator does not have permission to do.

Complete all end user tasks as well using Entrust Entelligence Security Provider.

- 1 The HR department advises you of the following new employees are starting with the company this Monday. Register the following new users in Entrust Authority Security Manager Administration and record the Reference Number and Authorization Code for each:
  - Heather Mantle
  - Gordon Dunn
  - Philip Sanders
  - Larry Bell
- 2 Heather Mantle activates her security store through Entrust Entelligence Security Provider.
- 3 Larry Bell activates his security store through Entrust Entelligence Security Provider.
- 4 Larry Bell encrypts a text file for himself.
- 5 Gordon Dunn calls HR and tells them he has accepted another position and will not coming to work for the company.
- 6 Heather calls and tells you she has forgotten the password for her security store. (Remember that this operation must be completed by Heather.)
- 7 Heather is taking a leave of absence for several months to get married. Your company policy states that employees should not be able to encrypt for people on leave. When employees return from leave, IT should be able to trust their certificate again.
- 8 Heather returns to work earlier than anticipated and needs to access her security store. As well, her married name is now Prescott. Company policy states that old Directory entries should be removed, but that a record of the old DNs should be kept in the new entries.
- 9 Your manager has asked you for a list of all the users that have not yet activated their security store. They would like the list in a tab delimited text file, showing only the user's DN.
- 10 You notice that Philip Sanders' activation codes have expired. You provide Philip with the new codes by phone. He activates his security store immediately after your phone call.
- 11 Larry Bell's mobile phone is stolen. He has written his security store password in a document stored on the device. Company policy states that in a scenario such as this, certificated must be revoked and new certificates created.
- 12 Larry Bell is dismissed from the company. His certificates must be made invalid. Company policy states that the accounts of departing employees should be removed from the database.
- 13 Larry's former manager discovers a file encrypted by Larry. He asks IT to decrypt the file.



## Distributing revocation information

This lab will provide you with a more practical look at revocation with digital identities.

## Lab

In these exercises, the default values for publishing revocation lists will be modified.

## Tasks

The following tasks will be completed:

Exercise 1: Verify the current revocation publishing values

Exercise 2: Modify the revocation publishing values

## Timing

Estimated time to complete these exercises is 30 minutes

## Exercise 1: Verify the current revocation publishing values

In this exercise, the default revocation publishing details will be verified.

- 1 Log into Entrust Authority Security Manager Master Control Command Shell as a Master User and enter the following command to review the default revocation publishing details:

```
rl config -query
```

## Exercise 2: Modify the revocation publishing values

In this exercise, the revocation publishing details will be updated.

- 1 Still logged into Entrust Authority Security Manager Master Control Command Shell as a Master User, enter the following command to update the publishing of the distributed CRL:

```
rl config -crl -life -hour 5 -preupdate -hour 1
```

What is the new lifetime of the distributed CRL? \_\_\_\_\_

How often will this CRL be updated? \_\_\_\_\_

- 2 Enter the following command to update the publishing of the combined CRL:

```
rl config -combined -life -day 2 -preupdate -hour 6
```

What is the new lifetime of the combined CRL? \_\_\_\_\_

How often will this CRL be updated? \_\_\_\_\_

- 3 Enter the following command to update the publishing of the ARL:

```
rl config -arl -life -hour 24 -preupdate -hour 1
```

What is the new lifetime of the ARL? \_\_\_\_\_

How often will this ARL be updated? \_\_\_\_\_

# Discussion Questions

- 1 Can a combined CRL have a different lifetime and update period from a partitioned CRL or ARL?
- 2 What maintenance is required on the OCSP responder?
- 3 What is OCSP stapling?

## General security policy

This lesson does not have a lab portion, but there are Discussion Questions.

# Discussion Questions

- 1 How can a user holding the Administrator role modify the policy settings regarding the lifetimes of cross-certificates?
- 2 What are some of the implications of enabling the **Allow DN reuse** policy setting?
- 3 What are some of the implications of removing expired certificates from the CRL?

## Client policies

In this lab you will create a new client policy, assign that policy to a role and register and activate a new end user with that role.

## Lab

In these exercises, a new client policy based on an existing policy will be created and some attributes of the policy will be modified. The new policy will be assigned to an existing role and the attribute changes tested.

### Tasks

The following tasks will be completed:

Exercise 1: Create a new client policy

Exercise 2: Assign the new client policy to a role

Exercise 3: Register and activate a new End User

### Timing

Estimated time to complete these exercises is 20 minutes

## Exercise 1: Create a new client policy

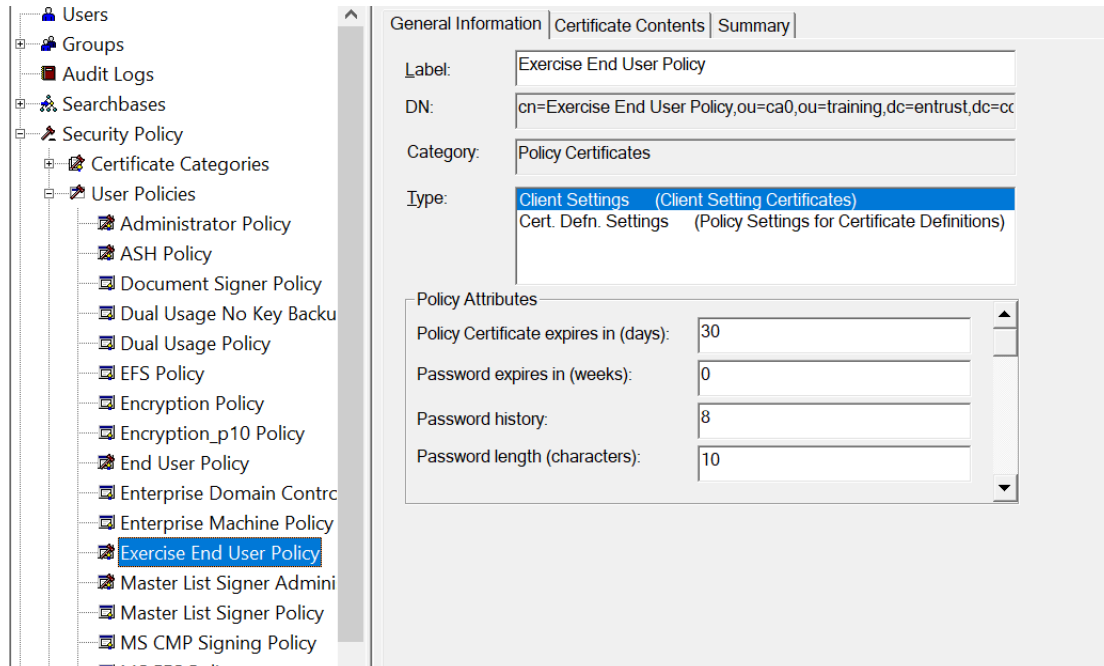
In this exercise, a new client policy will be created by copying an existing policy.

- 1 Log into Entrust Authority Security Manager as a Security Officer.
- 2 In the left-hand pane in Entrust Authority Security Manager, expand **Security Policy > User Policies**.
- 3 Right-mouse click the **End User Policy** and click **Copy**.
- 4 In the **Copy User Policy** dialog box, type the following:
  - **Label:** Type a name for the new policy, for example, `Exercise End User Policy`
  - **Common Name:** Type a common name for the policy. This represents the name the policy will be stored under in the Directory. The name used can be the same as the **Label**, for example, `Exercise End User Policy`
  - **Type:** Since a client policy was used as the basis for the copy, **Client Settings** will be selected in the Type list

- 5 Scroll through the list of **Policy Attributes** and make the following changes:
  - **Password length (characters):** 10
  - **Password needs non-alpha char:** Enable
  - **Password needs number:** Enable
  - **Login timeout:** 20
  - **Permit roaming:** Disable

Click **OK** to save the selected attributes and confirm by entering the Security Officer password when prompted.

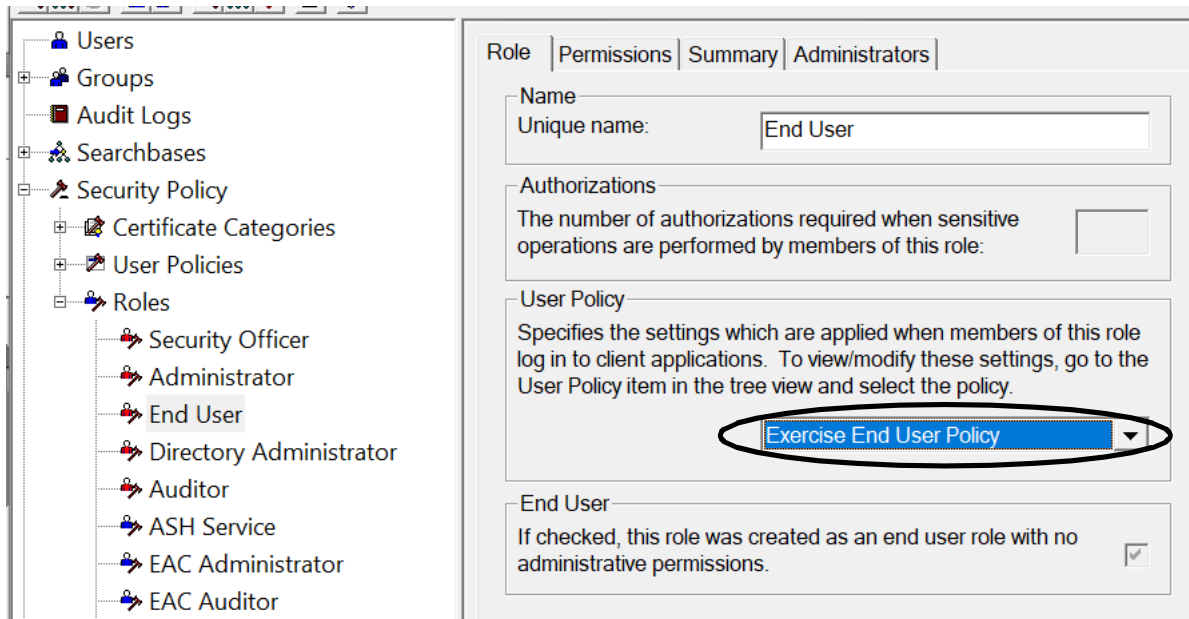
The new policy is displayed in the **User Policies** list.



## Exercise 2: Assign the new client policy to a role

Client policies are not applied directly to users. Instead, they are applied to a role, and the user is assigned that role. In this exercise, the new policy will be assigned to an existing role.

- 1 Still logged into Entrust Authority Security Manager Administration as a Security Office, expand **Security Policy > Roles**.
- 2 Click the **End User** role. In the right-hand pane, change the **User Policy** assigned to the default role to the policy created in Exercise 1 and click **Apply**.



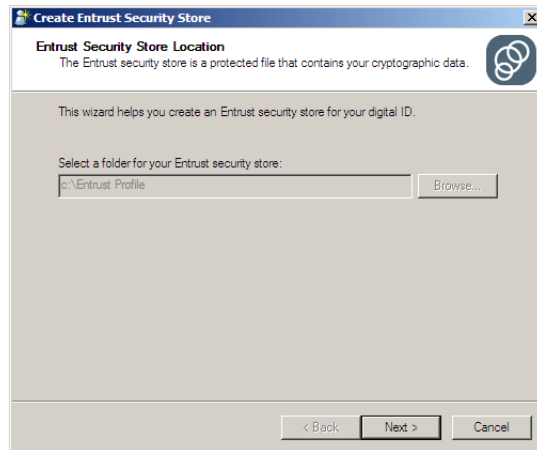
Authorize the operation with by typing the Security Officer password when prompted.

- 3 Log out of Entrust Authority Security Manager Administration as the Security Officer.

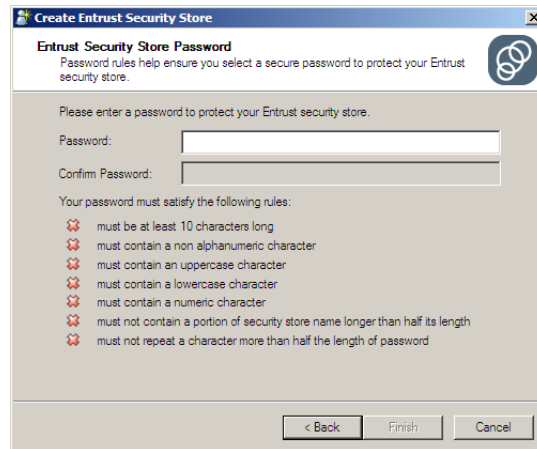
## Exercise 3: Register and activate a new End User

Any user assigned the End User role will now be bound by the attributes in the new client policy. In this exercise, a new user will be registered and their digital ID activated.

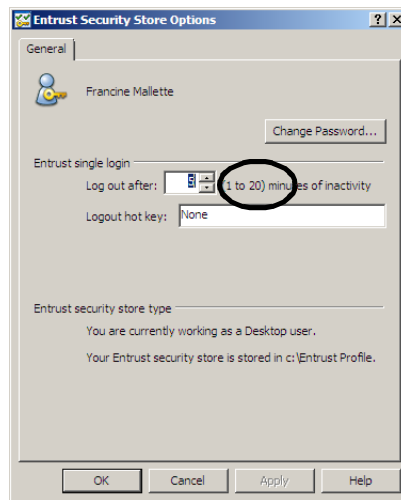
- 1 Log into Entrust Authority Security Manager Administration as an **Administrator**.
- 2 Register a new user in the default group and assign them the **End User** role and a **2-Key-Pair User** certificate type. Record the Reference Number and Authorization Code that is displayed.
- 3 Right-mouse click the Entrust Entelligence Security Provider icon and click **Enroll for Entrust Digital ID**. Step through the enrollment wizard.
- 4 Note that since roaming was disabled in the new policy, the user does not have the ability to select **In the Directory (work as a Roaming user)** when choosing a location for the security store.



- 5 Also note that when prompted to type a password for the security store, the new password attributes defined in the new policy are enforced. Type a password that conforms to the policy attributes and complete the creation of the security store.



- 6 Log into the security store as the new user. Right-mouse click the Entrust Entelligence Security Provider icon and click **Options**. Note that the maximum login timeout for this user is now set to 20 minutes as defined in the new policy.



- 7 Log back into Entrust Authority Security Manager Administration as the Security Officer and change the policy assigned to the End User role back to the default of End User Policy.
- 8 Log out of Entrust Authority Security Manager Administration.



## Roles and Administrative Permissions

This lab will give you hands on practice creating new roles and activating users with those roles to check permissions assigned.

## Lab

In these exercises, an existing role will be copied and modified permissions will be assigned to the new role. The role will be assigned to an administrative user and the permissions will be tested in Entrust Authority Security Manager Administration.

### Tasks

The following tasks will be completed:

Exercise 1: Create a new role

Exercise 2: Register and activate an Administrator with the new role

Exercise 3: Test the permissions assigned to the new role

### Timing

Estimated time to complete these exercises is 30 minutes

## Exercise 1: Create a new role

In this exercise, a new role will be created by copying an existing policy.

- 1 Log into Entrust Authority Security Manager as a Security Officer.
- 2 In the left-hand pane in Entrust Authority Security Manager, expand **Security Policy > Roles**.
- 3 Right-mouse click the **Administrator** role and click **Copy**.
- 4 In the role properties dialog box in the right-hand pane, type the following:
  - **Unique name:** Type a name for the new role, for example, `Classroom Administrator`
  - **Authorizations:** Type the number of authorizations the role holder will require to complete operations. Leave the authorizations value to the default of 1
  - **User Policy:** Select the **Client Policy** the new administrator will be bound by. Leave the setting as the default of **Administrator Policy**

The screenshot shows the 'Role Properties' dialog box with the 'Role' tab selected. The 'Name' field is empty. The 'Unique name' field contains 'Classroom Administrator'. The 'Authorizations' section shows 'The number of authorizations required when sensitive operations are performed by members of this role:' with a value of '1'. The 'User Policy' section shows 'Specifies the settings which are applied when members of this role log in to client applications. To view/modify these settings, go to the User Policy item in the tree view and select the policy.' with a dropdown menu set to 'Administrator Policy'. The 'End User' section shows 'If checked, this role will be created as an end user only role with no administrative permissions.' with an unchecked checkbox.

- 5 Click the **Permissions** tab and make the following changes to the **Users** category:
  - User - General
    - **Change DN:** disable

- **Revoke certificates:** disable

The screenshot shows the 'Administrative Permissions: Users' dialog box with the 'User - General' tab selected. The 'Permission' column lists various actions, and the 'Requires Authorization' column shows the status for each. The 'Revoke certificates' permission is unchecked and circled.

| Permission                                                   | Requires Authorization              |
|--------------------------------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> View                     | NA                                  |
| <input checked="" type="checkbox"/> Add                      | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Reactivate               | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Deactivate/Remove        | <input type="checkbox"/>            |
| <input type="checkbox"/> Change DN                           | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Modify properties        | <input type="checkbox"/>            |
| <input type="checkbox"/> Revoke certificates                 | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Update key pairs         | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Set for key recovery     | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Cancel key recovery      | <input type="checkbox"/>            |
| <input type="checkbox"/> Modify key update options           | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> View activation codes    | NA                                  |
| <input checked="" type="checkbox"/> Reissue activation codes | <input type="checkbox"/>            |

User - Advanced

- **Archive users:** Enable
- **Create user profile:** Enable

The screenshot shows the 'Administrative Permissions: Users' dialog box with the 'User - Advanced' tab selected. The 'Permission' column lists various actions, and the 'Requires Authorization' column shows the status for each. The 'Archive users' and 'Create user profile' permissions are checked and circled.

| Permission                                                               | Requires Authorization              |
|--------------------------------------------------------------------------|-------------------------------------|
| <input type="checkbox"/> Modify OIDs                                     | <input type="checkbox"/>            |
| <input type="checkbox"/> Change user's role                              | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Modify group membership              | <input type="checkbox"/>            |
| <input type="checkbox"/> Import new user                                 | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Export to another CA                            | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Archive users                        | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> View archived users                             | NA                                  |
| <input type="checkbox"/> Retrieve archived users                         | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Restore information to the Directory | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> Perform PKIX requests                | NA                                  |
| <input checked="" type="checkbox"/> Create user profile                  | NA                                  |
| <input type="checkbox"/> Recover user profile                            | NA                                  |
| <input type="checkbox"/> Convert Protocol Version                        | <input type="checkbox"/>            |

- 6 Click **OK**, then **Apply** to save the permissions and confirm by entering the Security Officer password when prompted.

- 7 The new role is displayed in the **Roles** list.

|                                |                                  |
|--------------------------------|----------------------------------|
| Roles                          | Self-Administration Server Admin |
| Security Officer               | User Administrator               |
| Administrator                  | User Reg Service (Admin Services |
| End User                       | Server Login                     |
| Directory Administrator        | EAC Auditor                      |
| Auditor                        | EAC Administrator                |
| ASH Service                    | EAC Self-Service                 |
| <b>Classroom Administrator</b> | EAC DV CKM Administrator         |
| EAC Administrator              | SPOC Role                        |
| EAC Auditor                    | SPOC Administrator               |
| EAC DV CKM Administrator       | SPOC Self-Service Role           |
| EAC Self-Service               | Master List Signer Administrator |
| Master List Signer Administra  | Modified Security Officer        |
| Modified Security Officer      | XAP Administrator                |
| Self-Administration Server Ac  | Classroom Administrator          |
| Server Login                   |                                  |

## Exercise 2: Register and activate an Administrator with the new role

Any user assigned the new administrator role will now be bound by the permissions in the role. In this exercise, a new administrator will be registered and their digital ID activated.

- 1 Still logged into Entrust Authority Security Manager Administration as a **Security Officer**, register a new user in the **default** group and assign them the new **Classroom Administrator**

role and a **2-Key-Pair User** certificate type. Record the Reference Number and Authorization Code that are displayed.

**New User**

Naming | General | Certificate Info | Key Update Options

User role: Classroom Administrator

User group(s):

☒ All groups

Available:

default

Assigned:

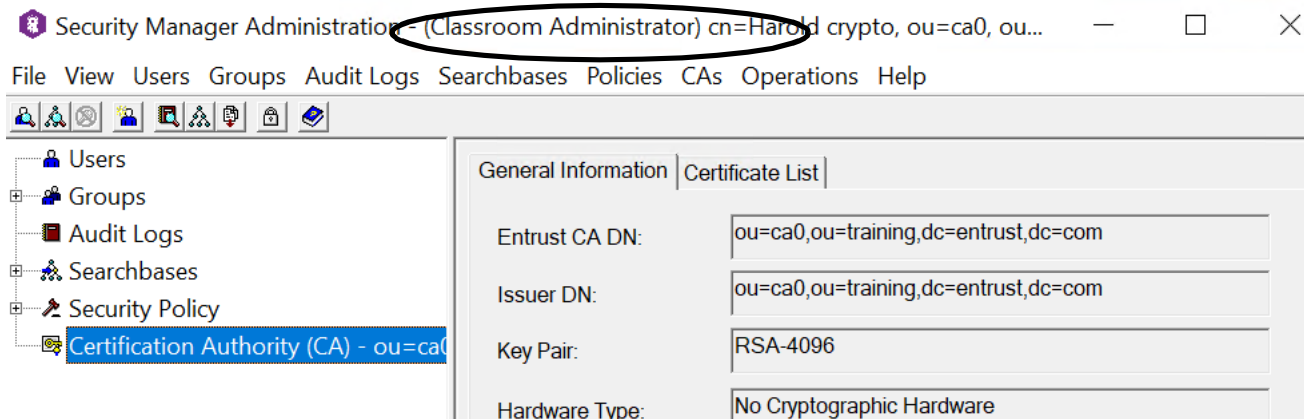
Add >>

<< Remove

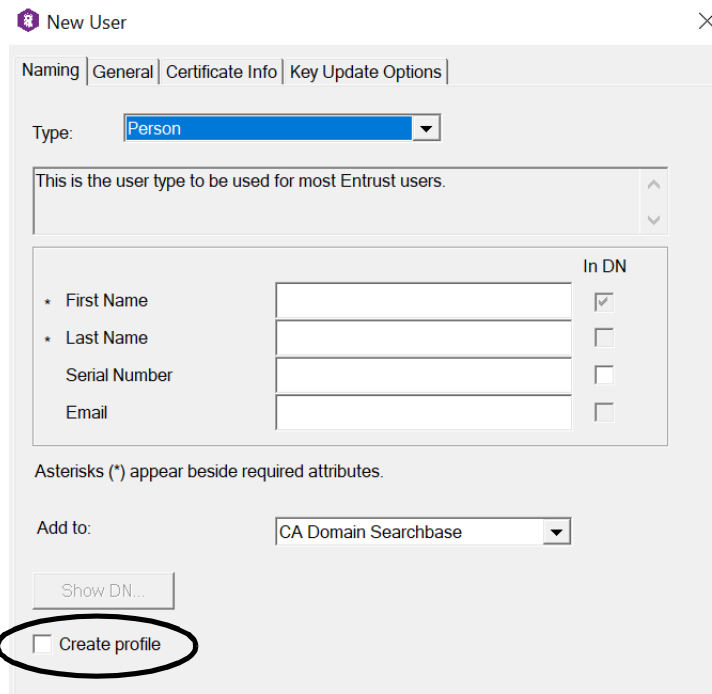
### Exercise 3: Test the permissions assigned to the new role

In this exercise, the permission changes applied to the new role will be tested.

- 1 Use Entrust Authority Security Manager Administration to create a profile for the newly created administrator and login. Note the role assigned to this administrator listed on the title bar of the program window.

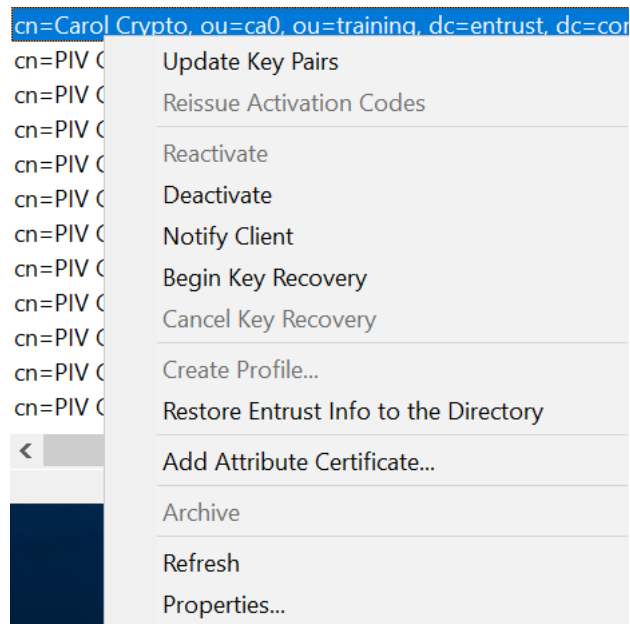


- 2 Click **New User** and note that the **Create profile** option is displayed on the **Naming** tab. The ability to create a desktop security store for another user is traditionally a permission only available when logged in as a Security Officer. We assigned this ability to the Classroom Administrator through the **Create Profile** permission. Click **Cancel** to close the **New User** dialog box.

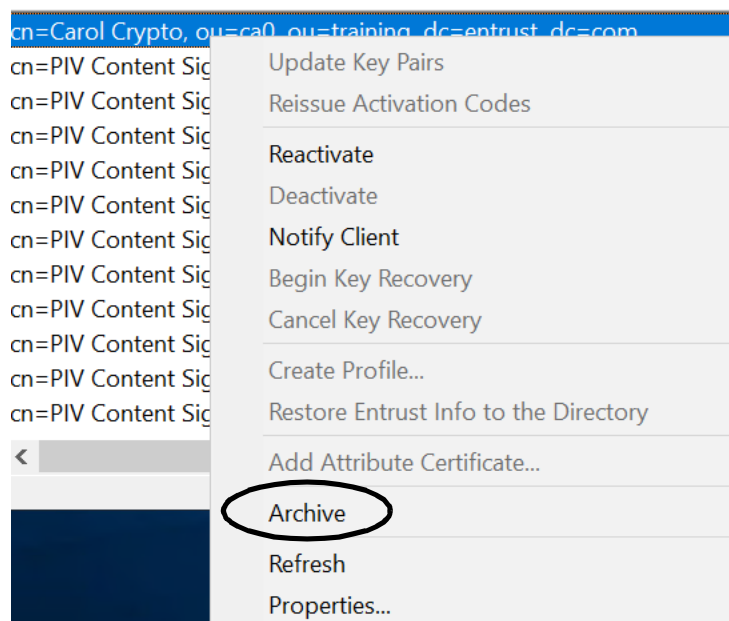


- 3 Perform a **Find** operation to locate the End Users registered in Entrust Authority Security Manager.

- 4 Right-mouse click an entry for an **Active** user and note that the **Change DN** operation is not displayed. The permission that allows an Administrator to change a user's distinguished name has been removed.

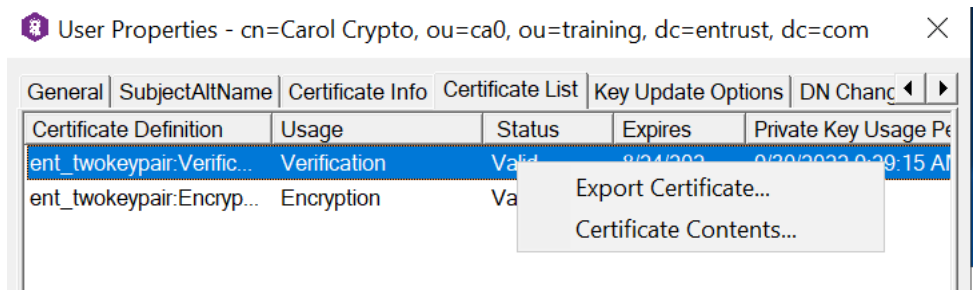


- 5 Right-mouse click an entry for an **Active** user and deactivate the user. Right-mouse click the entry for the deactivated user again and note that the **Archive** operation is available. The ability to archive a user is traditionally only available when logged in as a Security Officer. We assigned this ability to the Classroom Administrator through the **Archive users** permission.



- 6 Double-click an entry for an **Active** user to display the **User Properties** page and click the **Certificate List** tab. Right-mouse click one of the user's certificates and note that **Revoke**

**Certificates** is not available. The permission that allows an Administrator to revoke a certificate has been removed.



- 7 Log out of Entrust Authority Security Manager Administration as the Classroom Administrator.

## Lab

In this exercise, participants will rely on their knowledge of client policy and roles to complete the requirements of the scenario described below. Create the policies, roles, groups, users and any other items to satisfy the requirements and test that your solution is correct.

## Timing

Estimated time to complete these exercises is 45 minutes.

## Scenario

Your organization requires a specialized Help Desk role that will be assigned to agents providing telephone support to users. This role has certain requirements:

- Help Desk agents will only be able to perform operations to assist users who have forgotten the password on their security store. All other administrative operations unrelated to these operations should be disabled.
- Help Desk agents require a digital ID with three key pairs, including a non-repudiation key pair, stored in a desktop security store. These users must not be able to create their security store as a roaming profile.
- The security store must be protected by a 10 character password that includes a number. The password for the security store must be updated every 26 weeks and they cannot reuse any of the last six passwords used.
- For security purposes, if a Help Desk enters four consecutive incorrect password attempts within a one minute window, the login process should be terminated.

# Discussion Questions

- 1 What can a Security Officer do to create an administrative user that is prevented from creating new users but can manage existing users?
- 2 What method is available to the Security Officer to insure that they have not created a role with conflicting permissions?



## Certificate definition policies

In this lab you will create a new certificate definition policy, assign to policy to a certificate specification and register a new end user.

## Lab

In these exercises, a new certificate definition policy based on an existing policy will be created and some attributes of the policy will be modified. The new policy will be assigned to an existing certificate definition and the attribute changes tested.

### Tasks

The following tasks will be completed:

Exercise 1: Create a new certificate definition policy

Exercise 2: Assign the new certificate definition policy to a certificate specification

Exercise 3: Register and activate a new End User

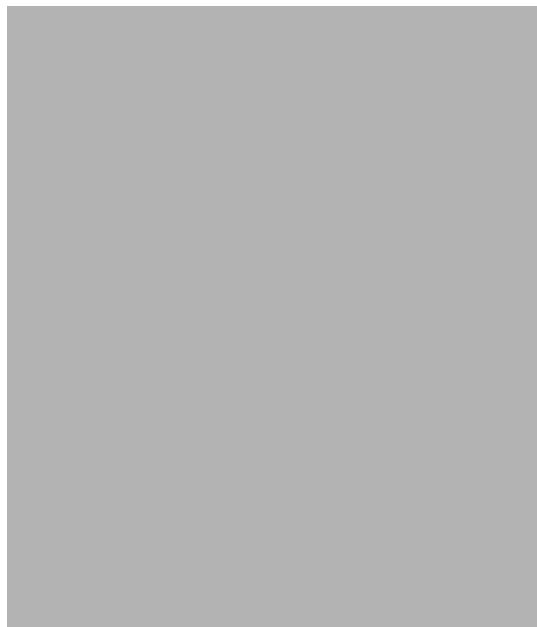
### Timing

Estimated time to complete these exercises is 20 minutes

## Exercise 1: Create a new certificate definition policy

In this exercise, a new certificate definition policy will be created by copying an existing policy.

- 1 Log into Entrust Authority Security Manager as a Security Officer.
- 2 In the left-hand pane in Entrust Authority Security Manager, expand **Security Policy > User Policies**.
- 3 Right-mouse click the **Encryption Policy** and click **Copy**.
- 4 In the **Copy User Policy** dialog box, type the following:
  - **Label:** Type a name for the new policy, for example, `Classroom Encryption Policy`
  - **Common Name:** Type a common name for the policy. This represents the name the policy will be stored under in the Directory. The name used can be the same as the **Label**, for example, `Classroom Encryption Policy`
  - **Type:** Since a client policy was used as the basis for the copy, **Cert. Defn. Settings** will be selected in the Type list



- 5 Scroll through the list of **Policy Attributes** and make the following changes:

- **Policy Certificate Expiry** 30
- **Certificate lifetime:** 24
- **Exclude entrustVersInfo:** Enable

Click **OK** to save the selected attributes and confirm by entering the Security Officer password when prompted.

The new policy is displayed in the **User Policies** list.

Security Manager Administration - (Security Officer) cn=Alice Admin, ou=ca0, ou=training, dc=entrust, dc=com

File View Users Groups Audit Logs Searchbases Policies CAs Operations Help

Users Groups Audit Logs Searchbases Security Policy Certificate Categories **User Policies**

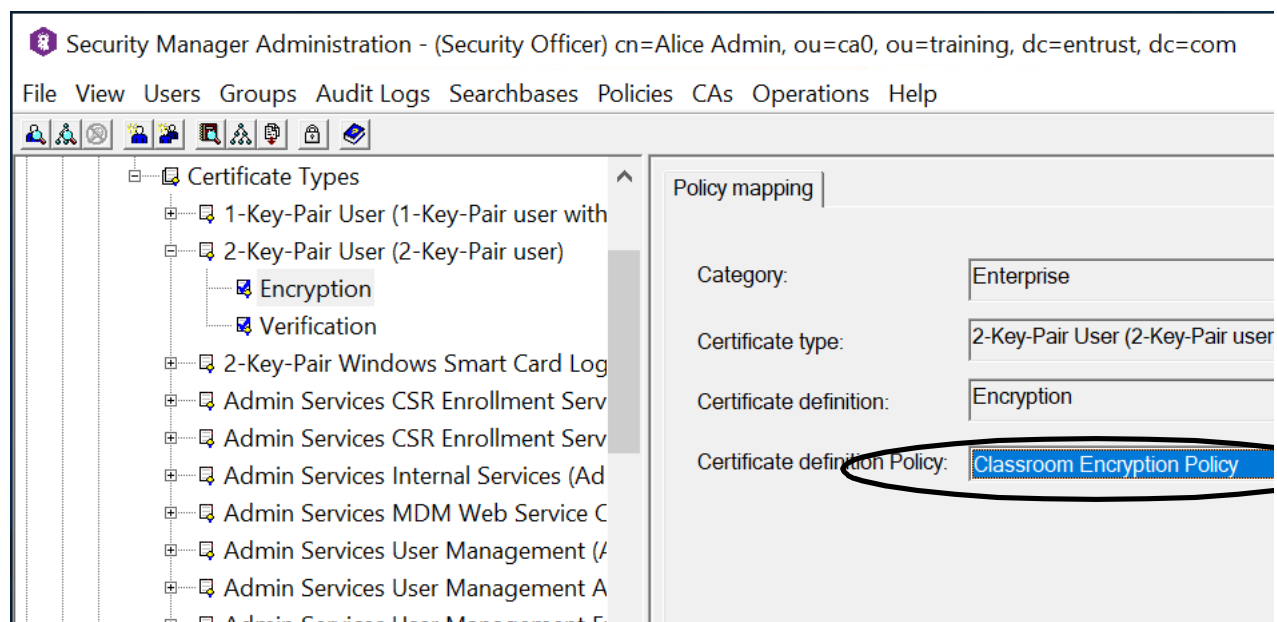
- Administrator Policy
- ASH Policy
- Classroom Encryption Policy**
- Document Signer Policy
- Dual Usage No Key Backup Policy
- Dual Usage Policy
- EFS Policy
- Encryption Policy
- Encryption\_p10 Policy
- End User Policy

| Label                                   | Cert Type        |
|-----------------------------------------|------------------|
| Administrator Policy                    | polcert_cliset   |
| ASH Policy                              | polcert_cliset   |
| Classroom Encryption Policy             | polcert_certdefn |
| Document Signer Policy                  | polcert_certdefn |
| Dual Usage No Key Backup Policy         | polcert_certdefn |
| Dual Usage Policy                       | polcert_certdefn |
| EFS Policy                              | polcert_certdefn |
| Encryption Policy                       | polcert_certdefn |
| Encryption_p10 Policy                   | polcert_certdefn |
| End User Policy                         | polcert_cliset   |
| Enterprise Domain Controller Policy     | polcert_certdefn |
| Enterprise Machine Policy               | polcert_certdefn |
| Exercise End User Policy                | polcert_cliset   |
| Master List Signer Administrator Policy | polcert_cliset   |
| Master List Signer Policy               | polcert_certdefn |
| MS CMP Signing Policy                   | polcert_certdefn |
| MS EFS Policy                           | polcert_certdefn |

## Exercise 2: Assign the new certificate definition policy to a certificate specification

Certificate definitions policies are not applied directly to users. Instead, they are applied to a certificate specification, and the user is assigned the certificate type that uses that specification. In this exercise, the new policy will be assigned to an existing certificate specification.

- 1 Still logged into Entrust Authority Security Manager Administration as a Security Office, expand **Security Policy > Certificate Categories > Enterprise > Certificate Types**.
- 2 Expand the **2-Key-Pair User** certificate type and click the **Encryption** definition. In the right-hand pane, change the **Certificate Definition Policy** assigned to the default definition to the **Exercise Encryption Policy** created in Exercise 1 and click **Apply**.



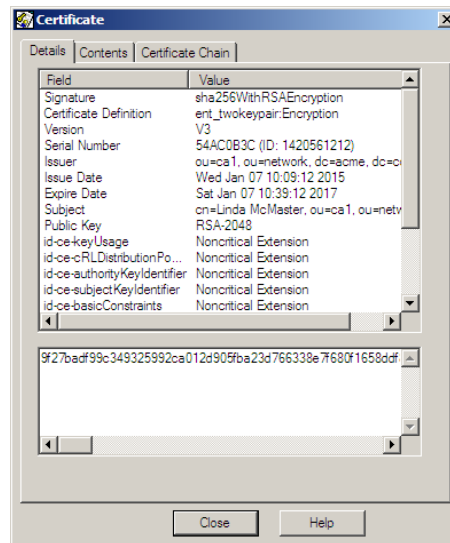
Authorize the operation with by typing the Security Officer password when prompted.

- 3 Log out of Entrust Authority Security Manager Administration as the Security Officer.

### Exercise 3: Register and activate a new End User

Any user assigned the 2-Key-Pair User certificate type will now be bound by the attributes in the new certificate definition policy. In this exercise, a new user will be registered and their digital ID activated.

- 1 Log into Entrust Authority Security Manager Administration as an **Administrator**.
- 2 Register a new user in the **default** group and assign them the **End User** role and a **2-Key-Pair User** certificate type. Record the Reference Number and Authorization Code that is displayed.
- 3 Right-mouse click the Entrust Entelligence Security Provider icon and click **Enroll for Entrust Digital ID**. Step through the enrollment wizard and activate the digital ID for the new user.
- 4 Return to Entrust Authority Security Manager Administration and locate the new user in the User List. Double-click the user entry to view the **User Properties**.
- 5 Click the **Certificate List** tab to view the user's certificates. Double-click the **Encryption** certificate to launch the **Certificate Viewer**.
- 6 Note that the life of the encryption certificate is now 24 months. Also, note that the **entrustVersInfo** extension has not been published in the certificate.



- 7 Click **Close** and log out of Entrust Authority Security Manager Administration.
- 8 Log back into Entrust Authority Security Manager Administration as the Security Officer and change the certificate definition policy assigned to the **2-Key-Pair User** certificate type back to the default of Encryption Policy.
- 9 Log out of Entrust Authority Security Manager Administration.

## Customizing certificate specifications

In this lab the certification specification file will be modified to add a new certificate type for an alternate 2-Key-Pair User. A new database field will also be defined for this new certificate type to allow the organization to store the user's location information in the Entrust Authority Security Manager database.

## Lab

In these exercises, the certification specification file will be modified to add a new certificate type for an alternate 2-Key-Pair User. A new database field will also be defined for this new certificate type to allow the organization to store the user's location information in the Entrust Authority Security Manager database.

### Tasks

The following tasks will be completed:

Exercise 1: Export the certificate specification file

Exercise 2: Modify the certificate specification file

Exercise 3: Import the modified certificate specification file

Exercise 4: Test the new certificate type

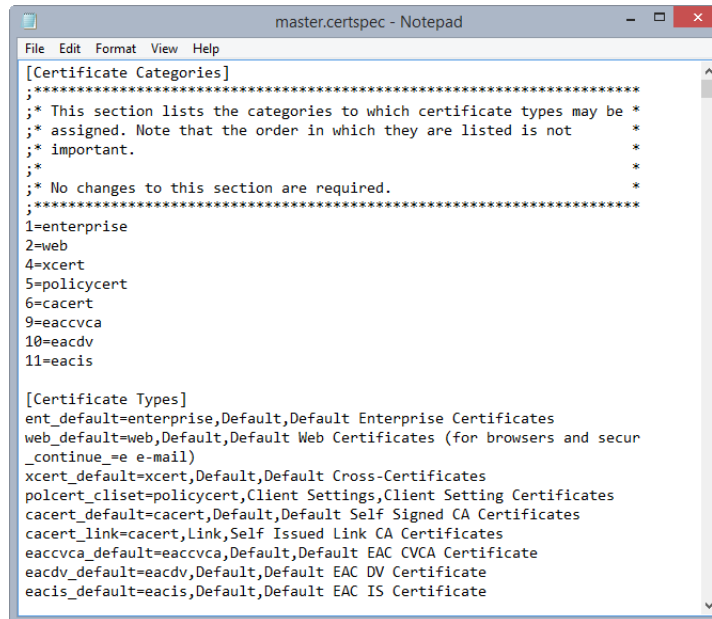
### Timing

Estimated time to complete these exercises is 45 minutes

## Exercise 1: Export the certificate specification file

In this exercise, the `master.certspec` file will be exported from Entrust Authority Security Manager.

- 1 Log into Entrust Authority Security Manager Administration as the Security Officer.
- 2 Click **File > Certificate Specifications > Export**. Save the file to the Windows desktop.
- 3 Open the `master.certspec` file in Windows Notepad.



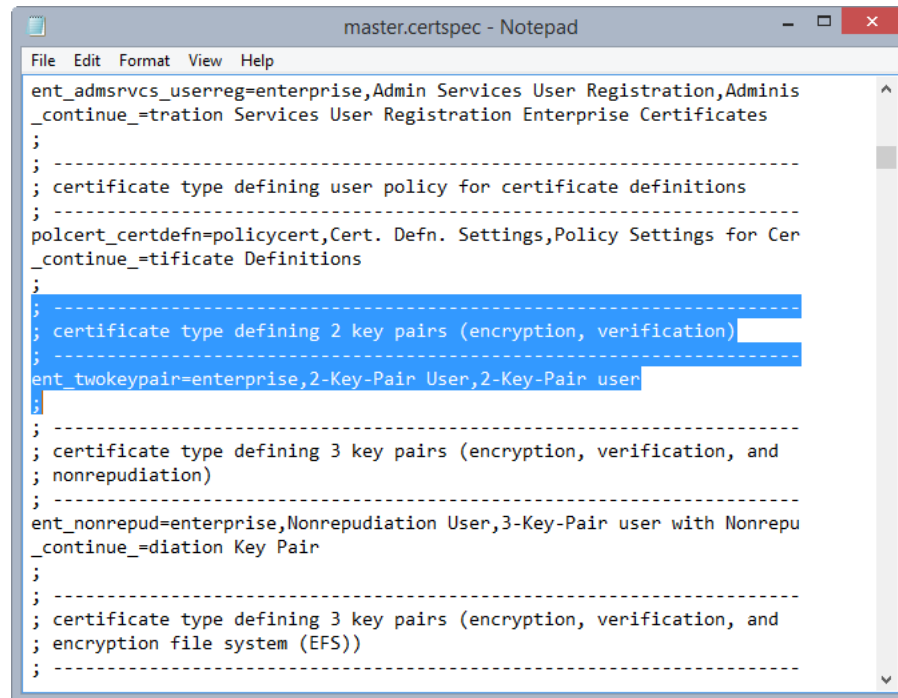
```
File Edit Format View Help
[Certificate Categories]
;*****
;* This section lists the categories to which certificate types may be *
;* assigned. Note that the order in which they are listed is not *
;* important. *
;* *
;* No changes to this section are required. *
;*****
1=enterprise
2=web
4=xcercert
5=policycert
6=cacert
9=eacccvca
10=eacdv
11=eacis

[Certificate Types]
ent_default=enterprise,Default,Default Enterprise Certificates
web_default=web,Default,Default Web Certificates (for browsers and secur
_continue_e e-mail)
xcercert_default=xcercert,Default,Default Cross-Certificates
polcert_cliset=policycert,Client Settings,Client Setting Certificates
cacert_default=cacert,Default,Default Self Signed CA Certificates
cacert_link=cacert,Link,Self Issued Link CA Certificates
eacccvca_default=eacccvca,Default,Default EAC CVCA Certificate
eacdv_default=eacdv,Default,Default EAC DV Certificate
eacis_default=eacis,Default,Default EAC IS Certificate
```

## Exercise 2: Modify the certificate specification file

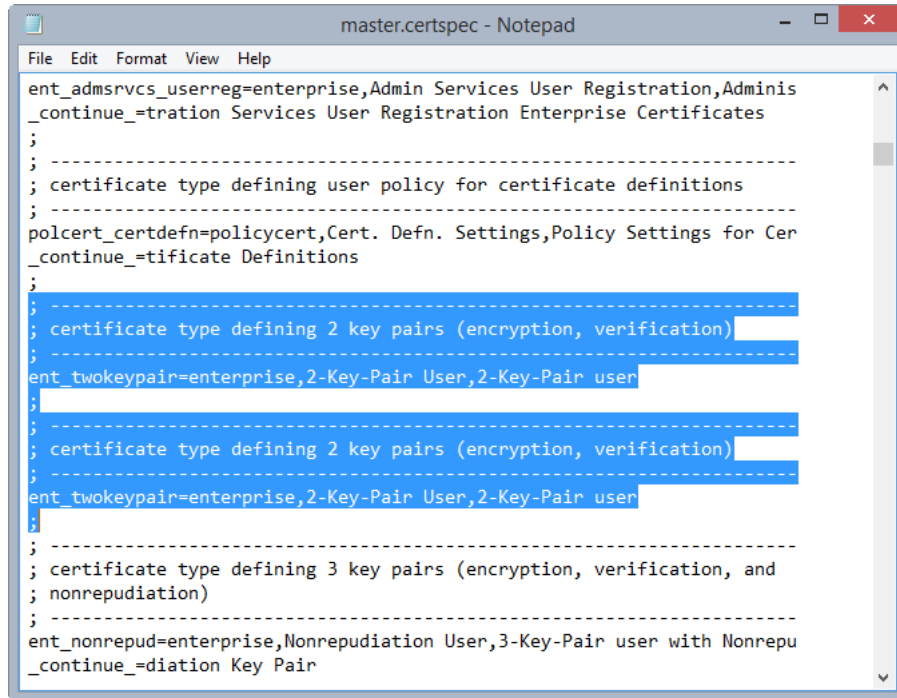
In this exercise, a new 2-Key-Pair User certificate type will be created by copying the default 2-Key-Pair User.

- 1 Scroll through the `master.certspec` file to locate the entry defining the 2-Key-Pair User certificate type.



```
ent_admsrvcs_userreg=enterprise,Admin Services User Registration,Adminis
continue=tration Services User Registration Enterprise Certificates
;
; -----
; certificate type defining user policy for certificate definitions
; -----
polcert_certdefn=policycert,Cert. Defn. Settings,Policy Settings for Cer
continue=tificate Definitions
;
; -----
; certificate type defining 2 key pairs (encryption, verification)
; -----
ent_twokeypair=enterprise,2-Key-Pair User,2-Key-Pair user
;
; -----
; certificate type defining 3 key pairs (encryption, verification, and
; nonrepudiation)
; -----
ent_nonrepud=enterprise,Nonrepudiation User,3-Key-Pair user with Nonrepu
continue=diation Key Pair
;
; -----
; certificate type defining 3 key pairs (encryption, verification, and
; encryption file system (EFS))
; -----
```

- 2 Copy the lines describing the certificate type and paste immediately after.



```
ent_admsrvcs_userreg=enterprise,Admin Services User Registration,Adminis
_continue=_tration Services User Registration Enterprise Certificates
;
; -----
; certificate type defining user policy for certificate definitions
; -----
polcert_certdefn=policycert,Cert. Defn. Settings,Policy Settings for Cer
_continue=_tificate Definitions
;
; -----
; certificate type defining 2 key pairs (encryption, verification)
; -----
ent_twokeypair=enterprise,2-Key-Pair User,2-Key-Pair user
;
; -----
; certificate type defining 2 key pairs (encryption, verification)
; -----
ent_twokeypair=enterprise,2-Key-Pair User,2-Key-Pair user
;
; -----
; certificate type defining 3 key pairs (encryption, verification, and
; nonrepudiation)
; -----
ent_nonrepud=enterprise,Nonrepudiation User,3-Key-Pair user with Nonrepu
_continue=_diation Key Pair
```

- 3 Modify the new section to the following:

```
; -----
; certificate type defining a new 2 key pair (encryption, verification)
; -----
ent_new_twokeypair=enterprise,New 2-Key-Pair User,Alt. 2-Key-Pair user
```

where:

- ent\_new\_twokeypair is the name used internally by Entrust Authority Security Manager to identify the new certificate type
- New 2-Key-Pair User is the label that will show up in the certificate type list
- Alt. 2-Key-Pair User is the description that will show up when the certificate type is selected

```

master.certspec - Notepad
File Edit Format View Help
ent_admsrvcs_userreg=enterprise,Admin Services User Registration,Adminis
continue=tration Services User Registration Enterprise Certificates
;
; -----
; certificate type defining user policy for certificate definitions
; -----
polcert_certdefn=policycert,Cert. Defn. Settings,Policy Settings for Cer
continue=tificate Definitions
;
; -----
; certificate type defining 2 key pairs (encryption, verification)
; -----
ent_twokeypair=enterprise,2-Key-Pair User,2-Key-Pair user
;
; -----
; certificate type defining a new 2 key pairs (encryption, verification)
; -----
ent_new_twokeypair=enterprise,New 2-Key-Pair User,Alt. 2-Key-Pair user
;
; -----
; certificate type defining 3 key pairs (encryption, verification, and
; nonrepudiation)
; -----
ent_nonrepud=enterprise,Nonrepudiation User,3-Key-Pair user with Nonrepu
continue=diation Key Pair

```

- 4 In the **[Extension Definitions]** section, locate the definition for the **ent\_twokeypair** certificate type.

```

master.certspec - Notepad
File Edit Format View Help
; encodes the entAdminServicesClients policy OID 2.16.840.1.114027.10.4
certificatepolicies=2.5.29.32,n,o,DER,300D300B06096086480186FA6B0A04

[ent_twokeypair Certificate Definitions]
;-----
;- Two Key-pair Certificate Type
;-
;- This certificate type defines two key pairs
;- Encryption: has keyEncipherment key usage bit set
;- Verification: has digitalSignature key usage bit set
;-
1=Encryption
2=Verification

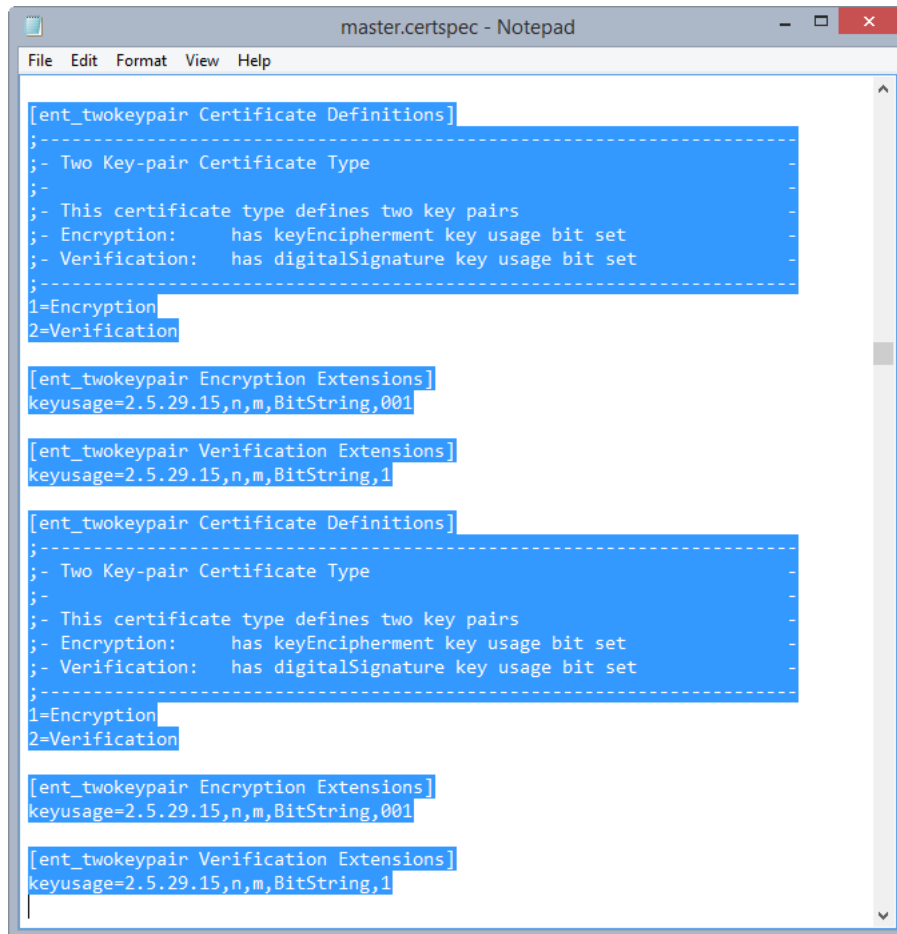
[ent_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_twokeypair Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1

[ent_nonrepud Certificate Definitions]
;-----
;- Nonrepudiation Certificate Type
;-
;- This certificate type defines three key pairs

```

- 5 Copy the entire section and paste immediate after.



```
[ent_twokeypair Certificate Definitions]

;- Two Key-pair Certificate Type
;-
;- This certificate type defines two key pairs
;- Encryption: has keyEncipherment key usage bit set
;- Verification: has digitalSignature key usage bit set
;-
1=Encryption
2=Verification

[ent_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_twokeypair Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1

[ent_twokeypair Certificate Definitions]

;- Two Key-pair Certificate Type
;-
;- This certificate type defines two key pairs
;- Encryption: has keyEncipherment key usage bit set
;- Verification: has digitalSignature key usage bit set
;-
1=Encryption
2=Verification

[ent_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_twokeypair Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1
```

- 6 Modify the new copied section to the following:

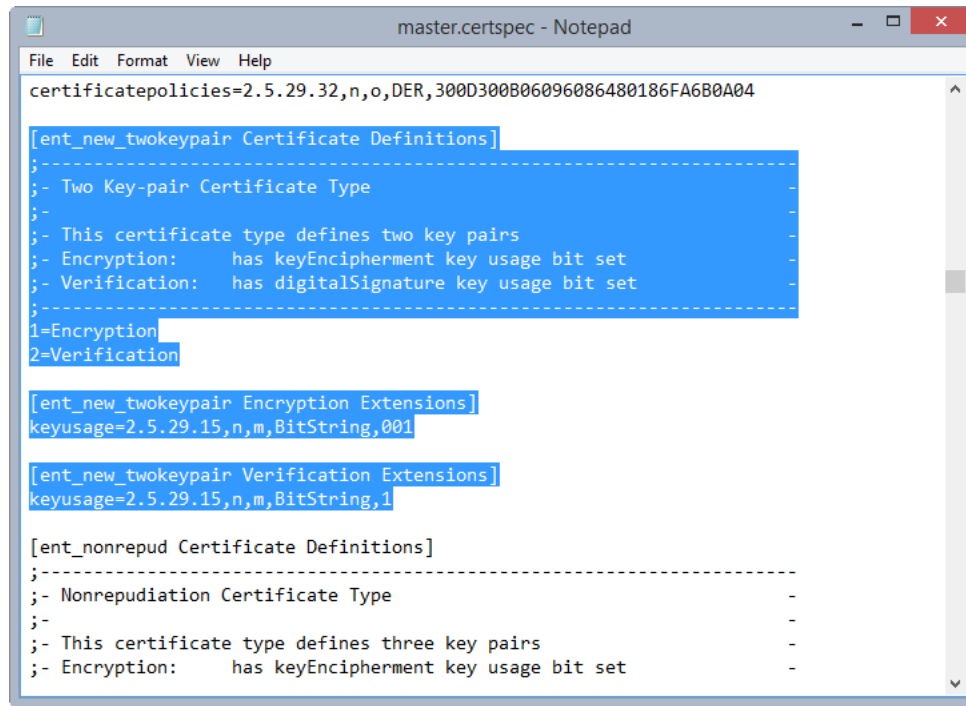
```
[ent_new_twokeypair Certificate Definitions]

;- Two Key-pair Certificate Type
;-
;- This certificate type defines a new two key pair user
;- Encryption: has keyEncipherment key usage bit set
;- Verification: has digitalSignature key usage bit set
;-
1=Encryption
2=Verification

[ent_new_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_new_twokeypair Verification Extensions]
```

keyusage=2.5.29.15,n,m,BitString,1



```
master.certspec - Notepad
File Edit Format View Help
certificatepolicies=2.5.29.32,n,o,DER,300D300B06096086480186FA6B0A04

[ent_new_twokeypair Certificate Definitions]
;-----
;- Two Key-pair Certificate Type
;-
;- This certificate type defines two key pairs
;- Encryption: has keyEncipherment key usage bit set
;- Verification: has digitalSignature key usage bit set
;-
1=Encryption
2=Verification

[ent_new_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_new_twokeypair Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1

[ent_nonrepud Certificate Definitions]
;-----
;- Nonrepudiation Certificate Type
;-
;- This certificate type defines three key pairs
;- Encryption: has keyEncipherment key usage bit set
```

- 7 Scroll down to the **[Database Field Definitions]** section and create a new entry as follows:

```
[ent_new_twokeypair Database Fields]
```

```
location=n,o,<location_var>
```

where:

- `location` is the name of the field in the database that will hold the value
- `n` indicates this is a non-secret value
- `o` indicates this is an optional value
- `<location_var>` is the value of the field, in this case, the value is derived from a variable defined in the **[Variables]** section

```

;* <Field Opt> *
;* This parameter specifies whether the variable upon which *
;* the database field's value depends is mandatory or *
;* optional. If mandatory, administrators must enter a value *
;* for the variable. If optional, no value will be stored for *
;* this database field. The value "o" indicates optional and *
;* "m" indicates mandatory. *
;* *
;* <Field Value> *
;* This parameter specifies the variable from which this *
;* database field is to derive its value. Administrators will *
;* be prompted to enter a value for this variable when *
;* enabling users with the given certificate type. *
;*****
[ent_new_twokeypair Database Fields]
location=n,o,<location_var>
;
[ent_default Database Fields]
;-----
;- Example Database Fields for Default Enterprise Certificate Type -
;-

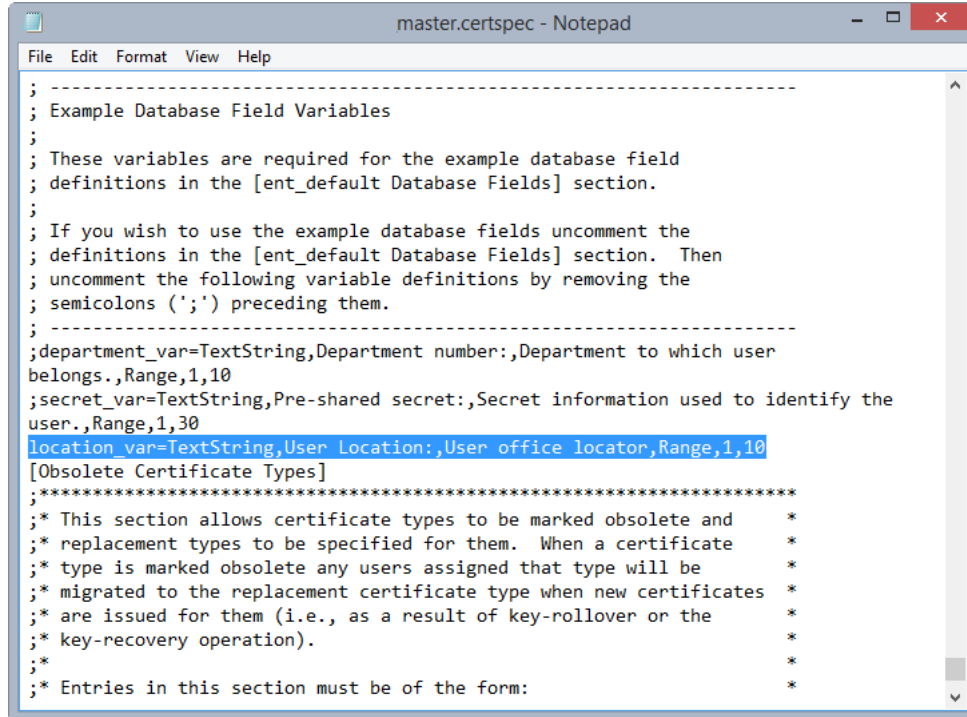
```

- 8 Continue scrolling to the **[Variables]** section and create a new entry at the end of the section as follows:

location\_var=TextString,User Location:,User office locator,Range,1,10

where:

- location\_var is the variable used for the value of the field
- TextString indicated the value will be treated as text
- User Location: is the name of the field displayed on the **Certificate Info** tab
- User office locator is the description displayed when the administrative user clicks in the field
- Range1,10 indicates the text can be between 1 and 10 characters long



```
; -----
; Example Database Field Variables
;
; These variables are required for the example database field
; definitions in the [ent_default Database Fields] section.
;
; If you wish to use the example database fields uncomment the
; definitions in the [ent_default Database Fields] section. Then
; uncomment the following variable definitions by removing the
; semicolons (';') preceding them.
; -----
;department_var=TextString,Department number:,Department to which user
;belongs.,Range,1,10
;secret_var=TextString,Pre-shared secret:,Secret information used to identify the
;user.,Range,1,30
location_var=TextString,User Location:,User office locator,Range,1,10
[Obsolete Certificate Types]
;*****
;* This section allows certificate types to be marked obsolete and *
;* replacement types to be specified for them. When a certificate *
;* type is marked obsolete any users assigned that type will be *
;* migrated to the replacement certificate type when new certificates *
;* are issued for them (i.e., as a result of key-rollover or the *
;* key-recovery operation). *
;* *
;* Entries in this section must be of the form: *
```

- 9 Save the master.certspec file.

## Exercise 3: Import the modified certificate specification file

In this exercise, the modifications to the `master.certspec` file will be applied to Entrust Authority Security Manager when the file is re-imported.

- 1 Still logged into Entrust Authority Security Manager Administration as the Security Officer, click **File > Certificate Specifications > Import**.
- 2 Locate the modified `master.certspec` file on the Windows desktop and click **Open**.
- 3 Accept the default log name displayed.

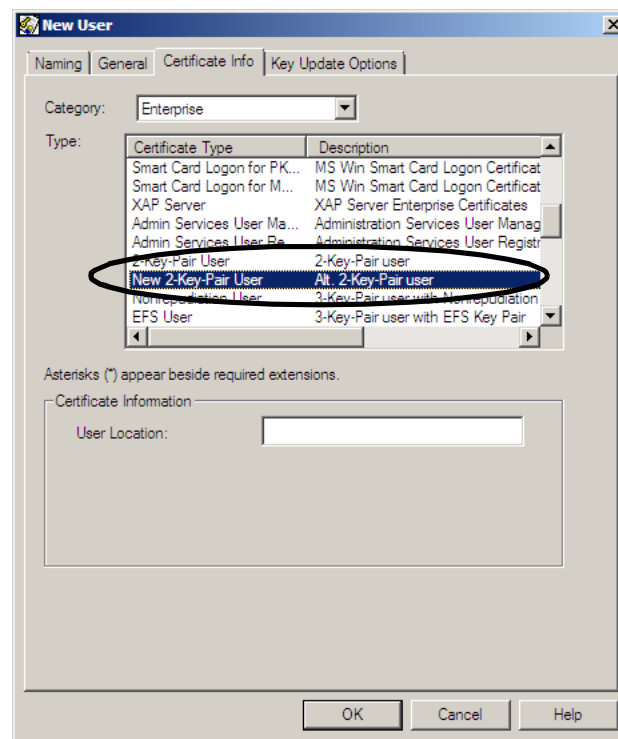
If no syntax errors were made in the file, the changes will be applied.

## Exercise 4: Test the new certificate type

In this exercise, the new certificate type and database field will be tested.

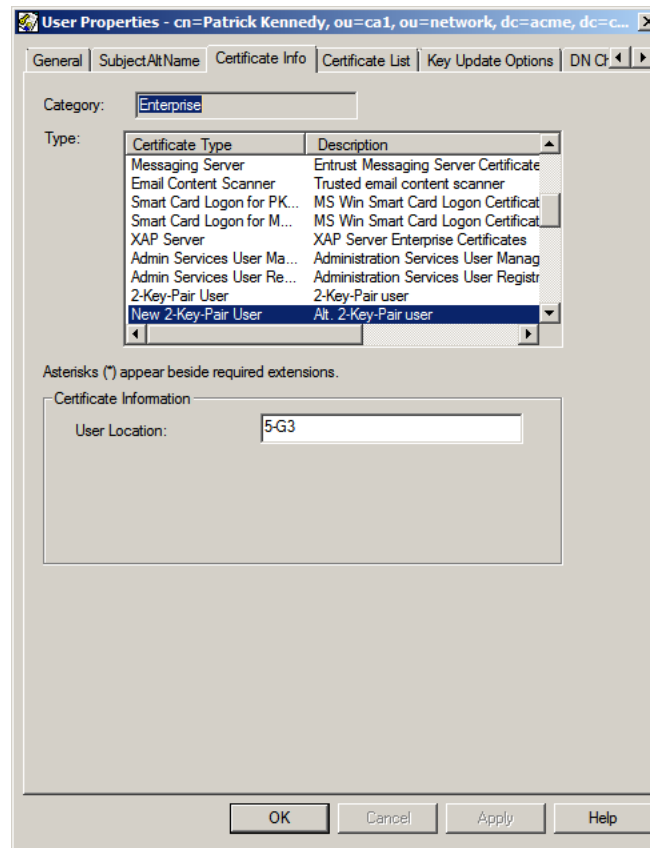
- 1 Still logged into Entrust Authority Security Manager Administration as the Security Officer, expand **Security Policy > Certificate Categories > Enterprise > Certificate Types** and locate the **New 2-Key-Pair User** certificate type created in the previous exercises.
- 2 Expand the **New 2-Key-Pair User** certificate type and click the certificate definition for the **Encryption** key pair. From the **Policy mapping** tab in the right-hand pane, select a **Certificate Definition Policy** from the list.
- 3 Repeat the same procedure for the **Verification** key pair.
- 4 Click **New User** and register a new End User.

On the **Certificate Info** tab, select the **New 2-Key-Pair User** certificate type and note that the new **User Location** database field is displayed. Complete the registration for the new user, making sure to add a value in the **User Location** field (the field was defined as holding up to 10 characters).



- 5 Activate the new end user in Entrust Entelligence Security Provider.

- 6 Perform a **Find** operation to locate the newly registered user and double-click the entry to view the **User Properties**. Note that the **User Location** information is displayed on the **Certificate Info** tab since the value is stored in the database along with the other user information.



- 7 Log out of Entrust Authority Security Manager Administration.



## Organizing users

This lab gives you hands on practice creating search bases and groups of users.

## Lab

In these exercises, participants will organize their community of users into groups. New groups will be created and existing users will be moved into the new groups. In addition, a new searchbase will be created and a new user will be added to this searchbase.

### Tasks

The following tasks will be completed:

Exercise 1: Create new groups

Exercise 2: Assign all existing users to groups

Exercise 3: Create a new searchbase

Exercise 4: Assign a new user to the searchbase

Exercise 5: Limit an administrator to a specific searchbase

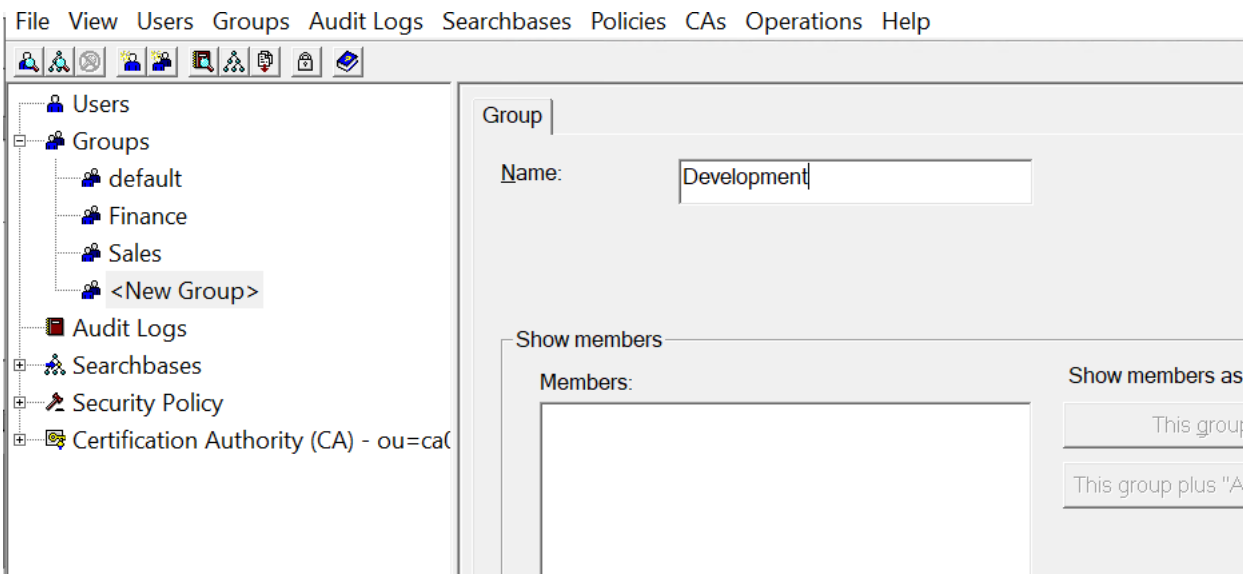
### Timing

Estimated time to complete these exercises is 30 minutes

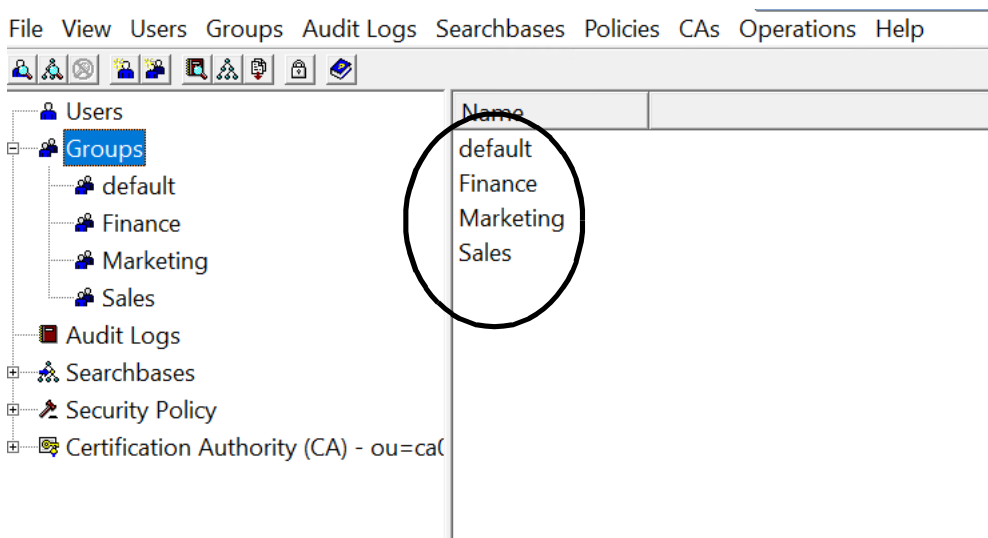
## Exercise 1: Create new groups

All users must belong to at least one group. In a default installation of Entrust Authority Security Manager, a group called **default** is created automatically and up to this point, all our users have been added to this group. In this exercise, new groups will be created.

- 1 Log into Entrust Authority Security Manager Administration as a Security Officer.
- 2 In the left-hand pane, right-mouse click **Groups** and click **New**.
- 3 On the **Group** tab in the right-hand pane, type a name for a new group and click **Apply**. Confirm the group creation by typing the Security Officer password.



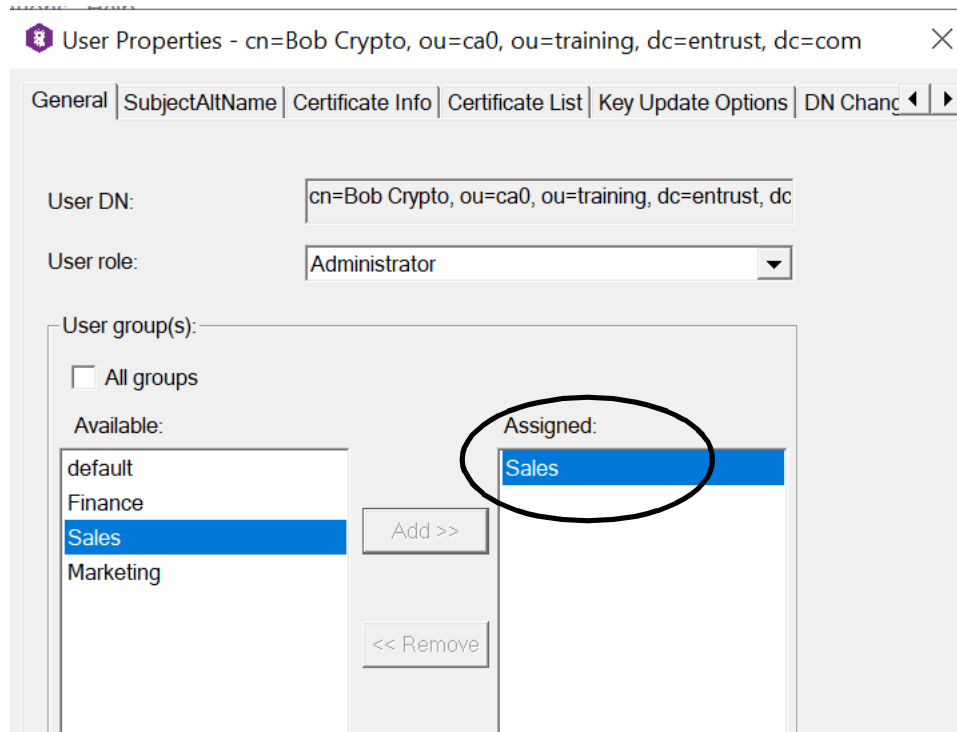
- 4 Right-mouse click **Groups** again, click **New** and create another new group.
- 5 Repeat the previous steps to create four new groups - Finance, Marketing, Development, Sales.



## Exercise 2: Assign all existing users to groups

The users previously added to the default group must be moved to the newly created groups. In this exercise, all users assigned to the default group will be moved into a specific group.

- 1 Still logged into Entrust Authority Security Manager as a Security Officer, perform a **Find** operation to list all the **End Users**.
- 2 Double-click each user entry to view the **User Properties**. On the **General** tab, assign the user to one of the new groups, and remove them from the **default** group.



- Repeat the previous steps so that no end users remain in the **default** group. In addition, if any **End Users** have been assigned to **All Groups**, deselect this option and assign them to a specific group.

Group | Administrators |

Name:

Show members

Added members:

cn=Carol Crypto, ou=ca0, ou=training, dc=entrust, d

Show members assigned to:

This group

This group plus "All groups"

Add members...

Remove member(s)

- Perform a **Find** operation once again, this time to list all the **Administrators**.
- Double-click each user entry to view the **User Properties**. On the **General** tab, assign the administrators to one of the new groups, and remove them from the **default** group.

User Properties - cn=Harold crypto, ou=ca0, ou=training, dc=entrust, dc=com

General | SubjectAltName | Certificate Info | Certificate List | Key Update Options | DN Chang

User DN:

User role:

User group(s):

☐ All groups

Available:

default

Finance

Sales

Marketing

Assigned:

Sales

Add >>

- Log into Entrust Authority Security Manager Administration as one of the administrators.

- 7 Click **New User** and register a new **End User**. Note that on the **General** tab, the Administrator is now limited to creating users within their own group.

- 8 Perform a **Find** operation again and note that the Administrator is only able to view users assigned membership in their own group.
- 9 Log out of Entrust Authority Security Manager Administration as the Administrator.

### Exercise 3: Create a new searchbase

A default searchbase was created when Entrust Authority Security Manager was initialized. This searchbase, called **CA Domain Searchbase** is the default location where user entries are created in the Directory tree. In this exercise, a new searchbase will be created.

- 1 Log into Entrust Authority Security Manager Administration as a Security Officer.
- 2 In the left-hand pane, right-mouse click **Searchbases** and click **New**.
- 3 Complete the **Searchbase Information** tab in the right-hand pane:
  - **Label:** Type a name for the new searchbase, for example, `Second searchbase`
  - **DN:** Type the distinguished name of a valid, existing branch in the Directory tree. A second Directory branch has been created for each user with the following DN:

`ou=ca, ou=production, dc=entrust, dc=com`

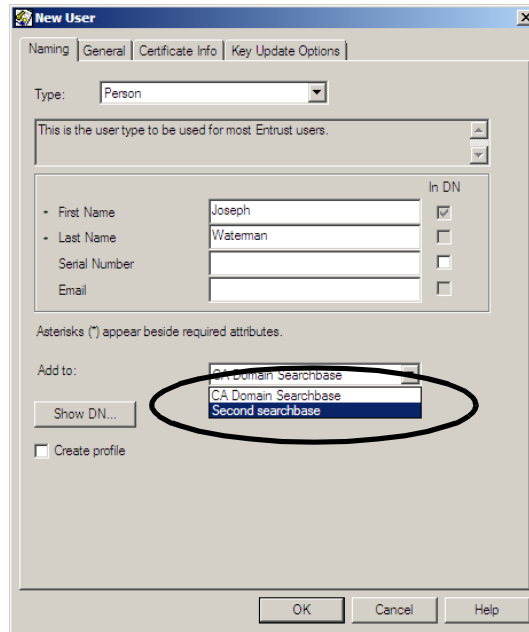


- 4 Click **Apply**.

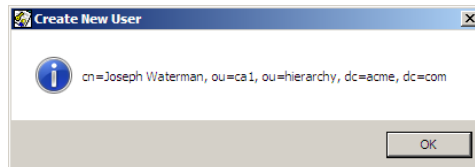
## Exercise 4:Assign a new user to the searchbase

In this exercise, a new user will be registered and their Directory entry created in the new searchbase.

- 1 Still logged into Entrust Authority Security Manager Administration as the Security Officer, click **New User** and register a new **End User**. Note that on the **Naming** tab that the new **Second Searchbase** appears in the **Add to** list.



- 2 Add the user to the new searchbase and click **Show DN** to display the distinguished name for the user. Note that the distinguished name is created using the selected searchbase. Click OK and complete the registration.



## Exercise 5:Limit an administrator to a specific searchbase

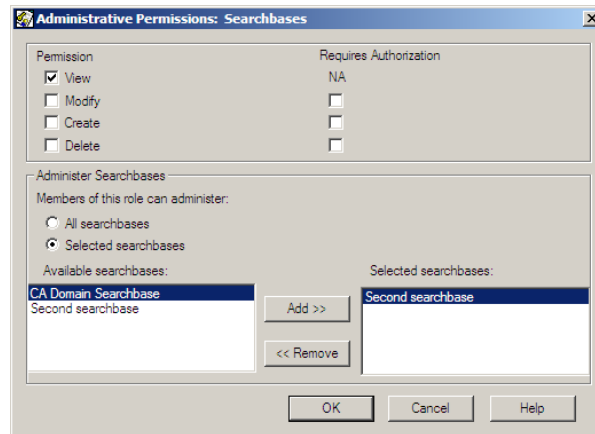
Permissions can be used to limit administrative users with a specific role to creating users only within specified searchbases. In this exercise, a new role with specific permission related to searchbases will be created and assigned to an existing administrator.

- 1 Still logged into Entrust Authority Security Manager Administration as the Security Officer, expand **Security Policy > Roles**.
- 2 Right-mouse click the **Administrator** role and click **Copy**.
- 3 In the role properties dialog box in the right-hand pane, type the following:
  - **Unique name:** Type a name for the new role, for example, `Second Searchbase Administrator`.
  - **Authorizations:** Type the number of authorizations the role holder will require to complete operations. Leave the authorizations value to the default of 1.

- **User Policy:** Select the **Client Policy** the new administrator will be bound by. Leave the setting as the default of **Administrator Policy**.
- 4 Click the **Permissions** tab and make the following changes to the **Searchbase** category:

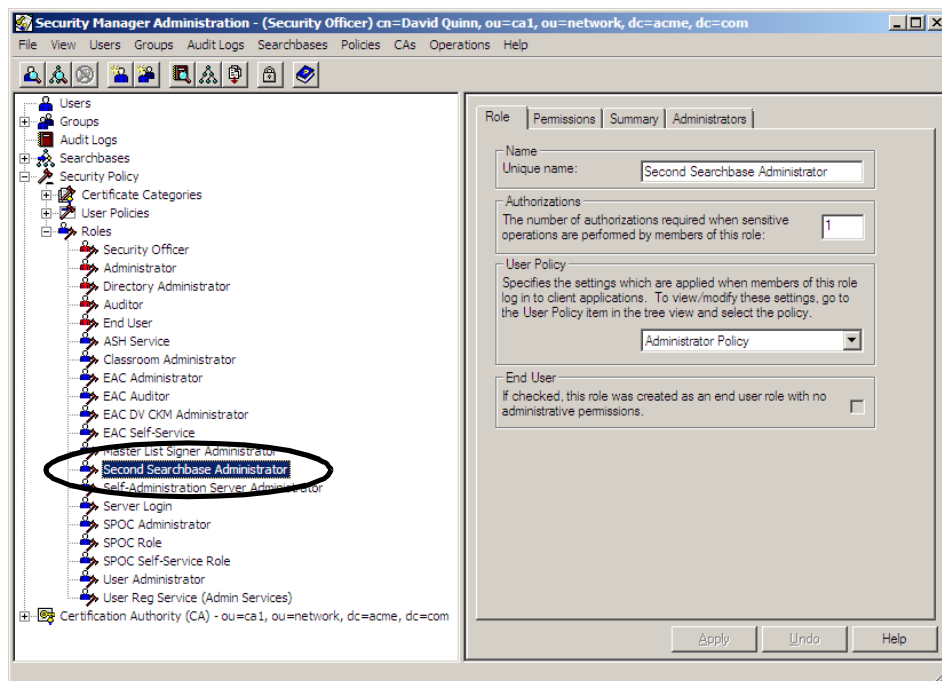
## Administer Searchbases

- **Selected searchbases:** move **Second searchbase** to the **Selected Searchbases** list



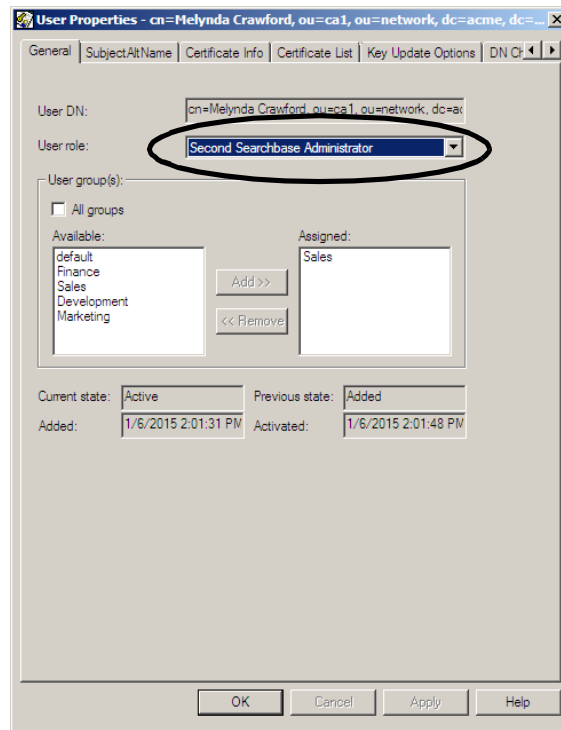
Click **OK**, then **Apply** to save the permissions and confirm by entering the Security Officer password when prompted.

The new role is displayed in the **Roles** list.

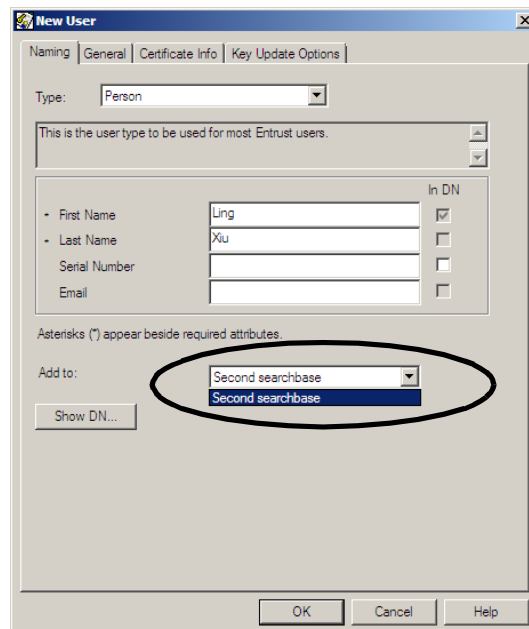


- 5 Perform a **Find** operation to list all the **Administrators**.

- 6 Double-click one of the administrative users to view their **User Properties**. On the **General** tab, change the role to the new **Second Searchbase Administrator** role, and click **OK**. Confirm the change by typing the Security Officer password.



- 7 Log into Entrust Authority Security Manager Administration as the modified Administrator.
- 8 Click **New User** and register a new **End User**. Since the searchbase permissions have been modified for this role, note that on the **Naming** tab, this administrator is only able to add this user to the **Second searchbase**.



- 9 Log out of Entrust Authority Security Manager Administration.

## Discussion Question

- 1 What are some of the differences between organizing the user community with groups compared to searchbases?





## Bulk operations

In this lab you will build and apply simple and more complex bulk operations.

## Lab

In these exercises, participants will create simple scripts to automate the registration of new End Users.

### Tasks

The following tasks will be completed:

Exercise 1: Register new users

Exercise 2: Deactivate user

Exercise 3: Update key pairs

Exercise 4: Register multiple users in a CSV file

### Timing

Estimated time to complete these exercises is 20 minutes

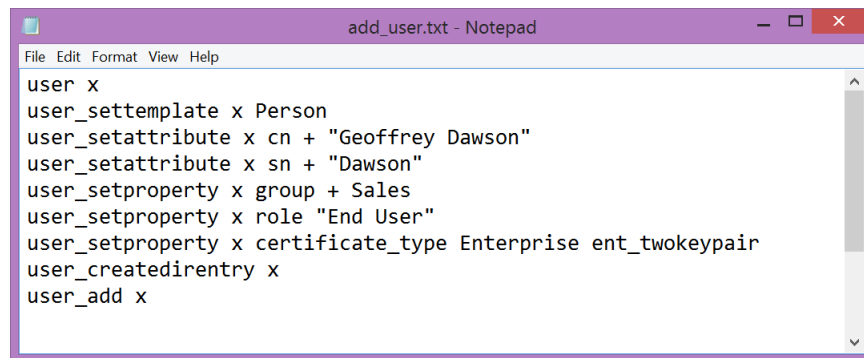
## Exercise 1: Register new users

In this exercise, you will write and execute a bulk script to register new End Users.

- 1 Create a new text file in Notepad and type the following commands to register a new End User:

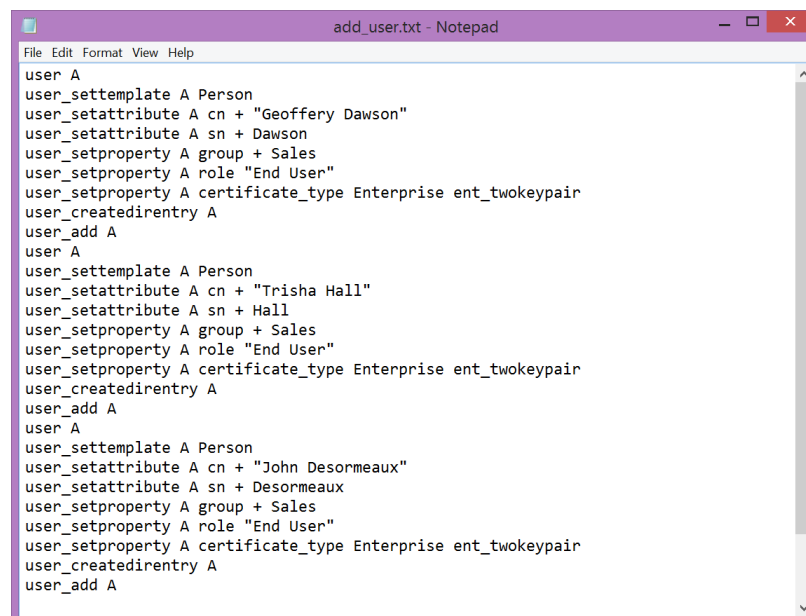
```
user x
user_settemplate x Person
user_setattribute x cn + "<First name> <Last name>"
user_setattribute x sn + <Last name>
user_setproperty x group + <Group name>
user_setproperty x role "End User"
user_setproperty x certificate_type Enterprise ent_twokeypair
user_createdirectory x
user_add x
```

(where <First name> is the first name of a new End User, <Last name> is the last name of a new End User and <Group name> is the name of a valid group in your configuration)



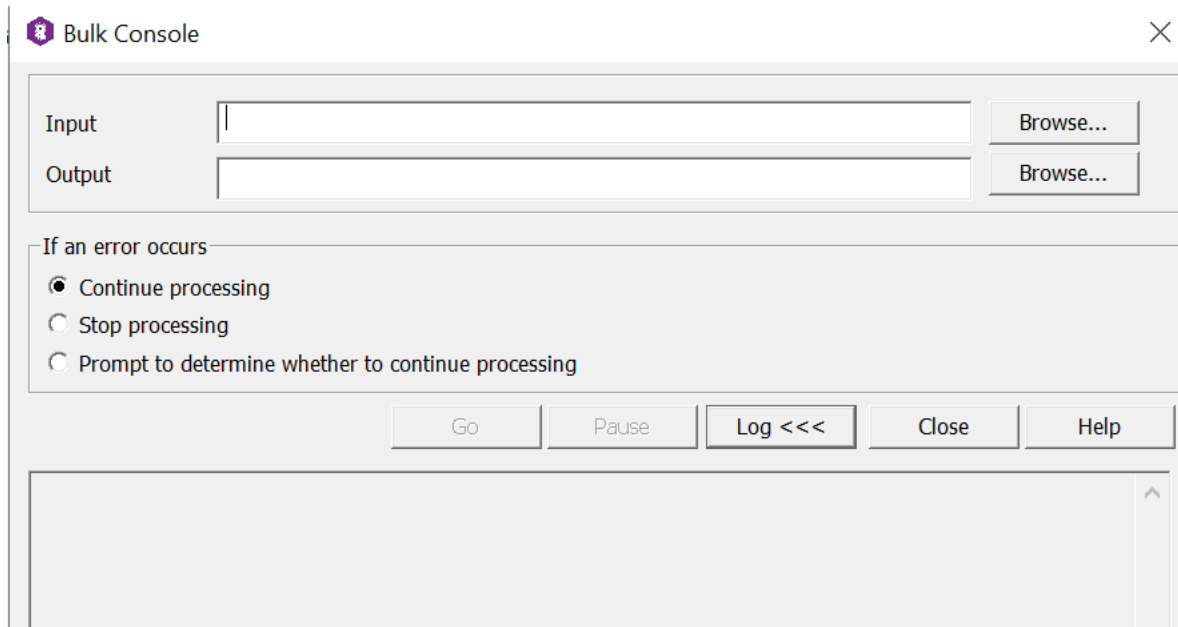
```
File Edit Format View Help
user x
user_settemplate x Person
user_setattribute x cn + "Geoffrey Dawson"
user_setattribute x sn + "Dawson"
user_setproperty x group + Sales
user_setproperty x role "End User"
user_setproperty x certificate_type Enterprise ent_twokeypair
user_createdirectory x
user_add x
```

- 2 Copy the lines you just typed and paste twice at the end of the file.
- 3 Modify the two sets of pasted lines to identify two more new End Users.



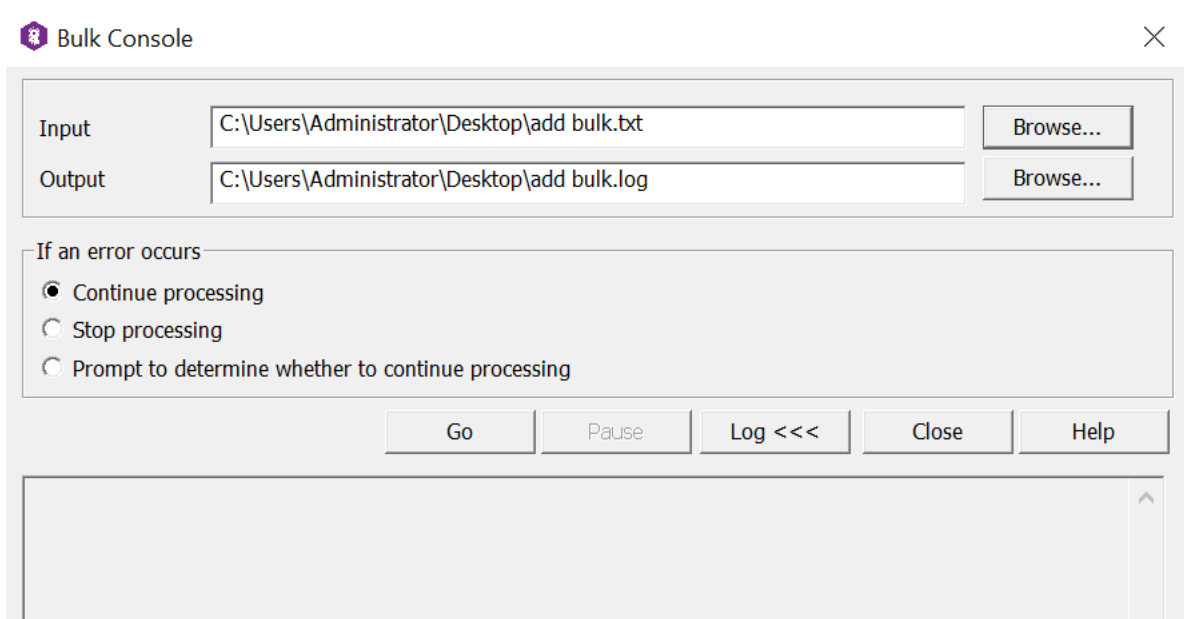
```
File Edit Format View Help
user A
user_settemplate A Person
user_setattribute A cn + "Geoffery Dawson"
user_setattribute A sn + Dawson
user_setproperty A group + Sales
user_setproperty A role "End User"
user_setproperty A certificate_type Enterprise ent_twokeypair
user_createdirectory A
user_add A
user A
user_settemplate A Person
user_setattribute A cn + "Trisha Hall"
user_setattribute A sn + Hall
user_setproperty A group + Sales
user_setproperty A role "End User"
user_setproperty A certificate_type Enterprise ent_twokeypair
user_createdirectory A
user_add A
user A
user_settemplate A Person
user_setattribute A cn + "John Desormeaux"
user_setattribute A sn + Desormeaux
user_setproperty A group + Sales
user_setproperty A role "End User"
user_setproperty A certificate_type Enterprise ent_twokeypair
user_createdirectory A
user_add A
```

- 4 Save the file.
- 5 Log in to Entrust Authority Security Manager Administration as an Administrator.
- 6 Click **Operations > Bulk Console**. The **Bulk Console** dialog box is displayed.



The Bulk Console dialog box is shown. It has a title bar with a gear icon and the text 'Bulk Console'. The main area contains two input fields: 'Input' and 'Output', each with a 'Browse...' button to its right. Below these is a section titled 'If an error occurs' with three radio buttons: 'Continue processing' (selected), 'Stop processing', and 'Prompt to determine whether to continue processing'. At the bottom are five buttons: 'Go', 'Pause', 'Log <<<', 'Close', and 'Help'. A large empty text area is at the very bottom.

- 7 Click **Browse** and locate the script file you just created.



The Bulk Console dialog box is shown again, but now the 'Input' field contains the path 'C:\Users\Administrator\Desktop\add bulk.txt' and the 'Output' field contains 'C:\Users\Administrator\Desktop\add bulk.log'. The 'If an error occurs' section remains the same, with 'Continue processing' selected. The buttons at the bottom are the same: 'Go', 'Pause', 'Log <<<', 'Close', and 'Help'.

- 8 Click **Stop processing** in the **If an error occurs** pane and click **Go**.

- 9 The completed steps of the script are listed in the **Bulk Console** window, along with the Reference Number and Authorization Code for each user.

Output

If an error occurs

☐ Continue processing

☒ Stop processing

☐ Prompt to determine whether to continue processing

```
[31/08/2020 15:15:15] user_setattribute :
 User with UserID x will be created using the Person template.
 Geoffrey Dawson added to cn for user x.
[31/08/2020 15:15:15] user_setattribute :
 Dawson added to sn for user x.
[31/08/2020 15:15:15] user_setproperty :
 Assign to group sales.
[31/08/2020 15:15:15] user_setproperty :
 Role End user assigned to user x.
[31/08/2020 15:15:15] user_setproperty :
 Set certificate category Enterprise and type ent_twokeypair for user x.
[31/08/2020 15:15:15] user_createdirectoryentry :
 Directory entry created for UserID x.
 User DN is cn=Geoffrey Dawson, ou=ca0, ou=training, dc=entrust, dc=com.
[31/08/2020 15:15:21] user_add :
 Added user cn=Geoffrey Dawson, ou=ca0, ou=training, dc=entrust, dc=com to Entrust.
 Reference number: 76688701
 Authorization code: SGPF-LUI9-CCAG.
[31/08/2020 15:15:21] C:\Users\Administrator\Desktop\add bulk.txt :
 Processing complete.
```

## Exercise 2: Deactivate user

In this exercise, you will create and execute a script to deactivate a user.

- 1 Use the **Find** operation to locate an **Active** user in Entrust Authority Security Manager Administration and note their DN.
- 2 Create and execute a script file to deactivate this user using the following command:

```
user_deactivate
```

## Exercise 3:Update key pairs

In this exercise, you will create and execute a script to update the key pairs for a user.

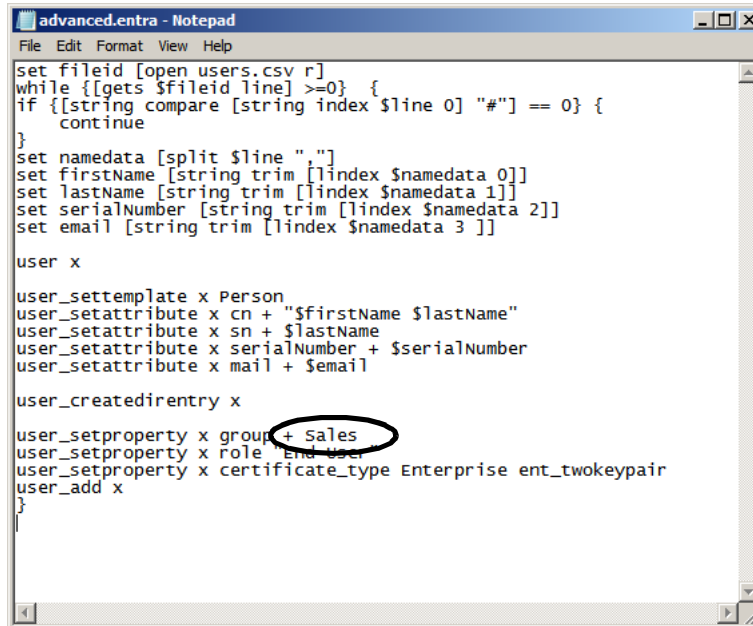
- 1 Locate another **Active** user and note their DN.
- 2 Create and execute a script file to set this user for key update using the following command:

```
user_updatekeypairs
```

## Exercise 4: Register multiple users in a CSV file

In this exercise, an example of advanced TCL scripting will be examined.

- 1 Locate the `advanced.entra` file in the `...Source\Classroom Support Files\Bulk Script` folder and open in Notepad. Review the script steps.
- 2 Modify the entry setting the group property to use a valid group in your infrastructure and save the file.



```
advanced.entra - Notepad
File Edit Format View Help
set fileid [open users.csv r]
while {[gets $fileid line] >= 0} {
 if {[string compare [string index $line 0] "#" == 0]} {
 continue
 }
 set namedata [split $line " "]
 set firstName [string trim [lindex $namedata 0]]
 set lastName [string trim [lindex $namedata 1]]
 set serialNumber [string trim [lindex $namedata 2]]
 set email [string trim [lindex $namedata 3]]

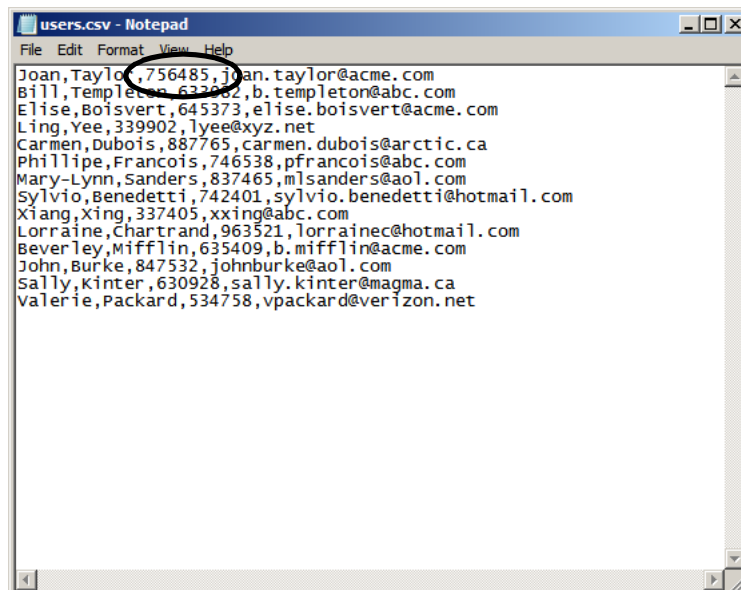
 user x

 user_settemplate x Person
 user_setattribute x cn + "$firstName $lastName"
 user_setattribute x sn + $serialNumber
 user_setattribute x serialNumber + $serialNumber
 user_setattribute x mail + $email

 user_createdirentry x

 user_setproperty x group + Sales
 user_setproperty x role "End User"
 user_setproperty x certificate_type Enterprise ent_twokeypair
 user_add x
}
```

- 3 Locate the `user.csv` file in the same folder. Open the file in Notepad and overwrite the serial number with a unique value **for each user**. Save the file when finished.



```
users.csv - Notepad
File Edit Format View Help
Joan,Taylor,756485,joan.taylor@acme.com
Bill,Templeton,632082,b.templeton@abc.com
Elise,Boisvert,645373,elise.boisvert@acme.com
Ling,Yee,339902,lyee@xyz.net
Carmen,Dubois,887765,carmen.dubois@arctic.ca
Phillipe,Francois,746538,pfrancois@abc.com
Mary-Lynn,Sanders,837465,mlsanders@aol.com
Sylvio,Benedetti,742401,sylvio.benedetti@hotmail.com
Xiang,Xing,337405,xxing@abc.com
Lorraine,Chartrand,963521,lorrainec@hotmail.com
Beverley,Mifflin,635409,b.mifflin@acme.com
John,Burke,847532,johnburke@aol.com
Sally,Kinter,630928,sally.kinter@magma.ca
Valerie,Packard,534758,vpackard@verizon.net
```



**Note:**

The Directory used in the classroom requires that serial numbers be unique within the **entire Directory**. For this reason, each participant must overwrite the serial numbers in the file with unique values to prevent conflicts with others in the classroom.

---

- 4 Run the script and observe the processing in the **Bulk Console** window.
- 5 Perform a **Find User** operation in Entrust Authority Security Manager Administration and verify that the users have been registered.
- 6 Log out of Entrust Authority Security Manager Administration.

## Discussion Questions

- 1 What is an way for an administrative user to create a text file of with the names of users in a particular state on which to perform bulk operations?

## Logging and reporting

In this lab you will discover where the logs are and view details from the weeks activities, and create a few predefined reports.

## Lab

In these exercises, participants will use the audit logs to locate operations that have taken place in Entrust Authority Security Manager. In addition, a sample report will be generated.

### Tasks

The following tasks will be completed:

Exercise 1: Locate administrative operations

Exercise 2: Generate a report of future expiring certificates

### Timing

Estimated time to complete these exercises is 20 minutes

## Exercise 1: Locate administrative operations

In this exercise, a Security Officer will use the audit logs to locate operations that have been performed in Entrust Authority Security Manager.

- 1 Log into Entrust Authority Security Manager Administration as a Security Officer.
- 2 Click **Audit Logs > Search** and use the logging details to answer the following questions:
  - How many times has Master1 logged into Entrust Authority Security Manager Control Command Shell since the Certification Authority was initialized?
  - When was the last time a CRL was published to the Directory?
  - Which operations occurred between 9am and noon on Wednesday of this week?
  - How many Enterprise licenses are currently in use in your infrastructure
  - Have any ALARM events occurred since Entrust Authority Security Manager was initialized?

## Exercise 2: Generate a report of future expiring certificates

In this exercise, a report will be generated to identify any certificates that have expired.

- 1 Still logged into Entrust Authority Security Manager Administration as a Security Officer, click **Operations > Create Report**
- 2 Click the **Certificates** tab and configure a search with the following properties:
  - **Certificate Category:** Enterprise
  - **Certificate Type:** 2-Key-Pair
  - **Expired:** <Latest expired>

Create Report

General Certificates State History Range Report Type

Certificate Category: Enterprise

Certificate Type: 2-Key-Pair User (2-Key-Pair user)  
Nonrepudiation User (3-Key-Pair user)  
EFS User (3-Key-Pair user with EFS)  
Standalone EFS User (2-Key-Pair user)

Revoked: < Any >

Expired: <Latest expired>

Signing Usage Ends: < Any >

Issued: < Any >

Policy: < Any >

☐ Key Update Pending



## Cross-certification

In this lab you will Explore Cross-certification options.

## Lab

In these exercises, cross-certification options will be explored

### Tasks

The following tasks will be completed:

Exercise 1: Backup the current configuration

Exercise 2: Create the cross-certification request

Exercise 3: Complete an offline cross-certification

### Timing

Estimated time to complete these exercises is 15 minutes

## Exercise 1: Backup the current configuration

Before any cross-certification is done a full backup will be performed.

- 1 Log into Entrust Authority Security Manager Control Command Shell as a Master User and type the following command:

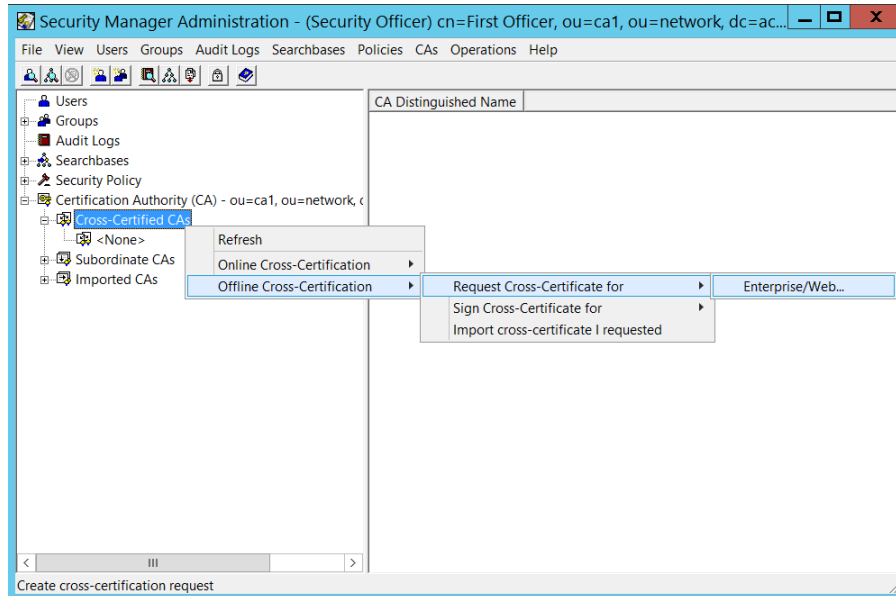
```
db backup full
```

- 2 When the backup shows as complete, close Entrust Authority Security Manager Control Command Shell.

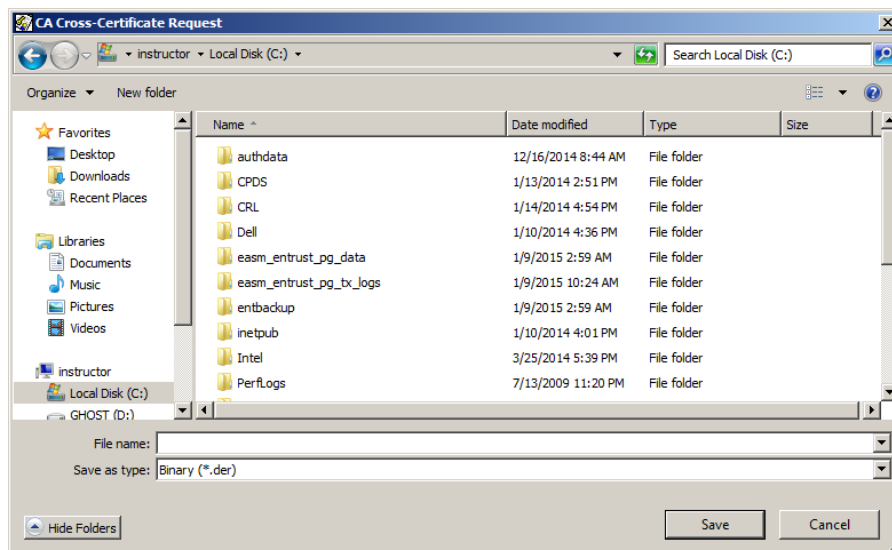
## Exercise 2: Create the cross-certification request

In this exercise, the Security Officer will create a cross-certification request.

- 1 Log in to Entrust Authority Security Manager Administration as a Security Officer.
- 2 In the left-hand pane, expand **Certification Authority** and right-click **Cross-Certified CAs**.
- 3 Click **Offline Cross-Certification > Request Cross-Certificate for > Enterprise/Web**.

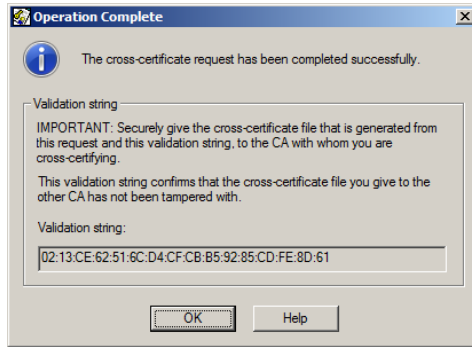


- 4 Save the **cross-certificate request** to a destination folder. The certificate request will be saved in a file with a \*.der extension



- 5 Authorize the activity by typing the Security Officer password.

- 6 An **Operation Complete** message box appears showing a **Validation string**. Click **OK**.

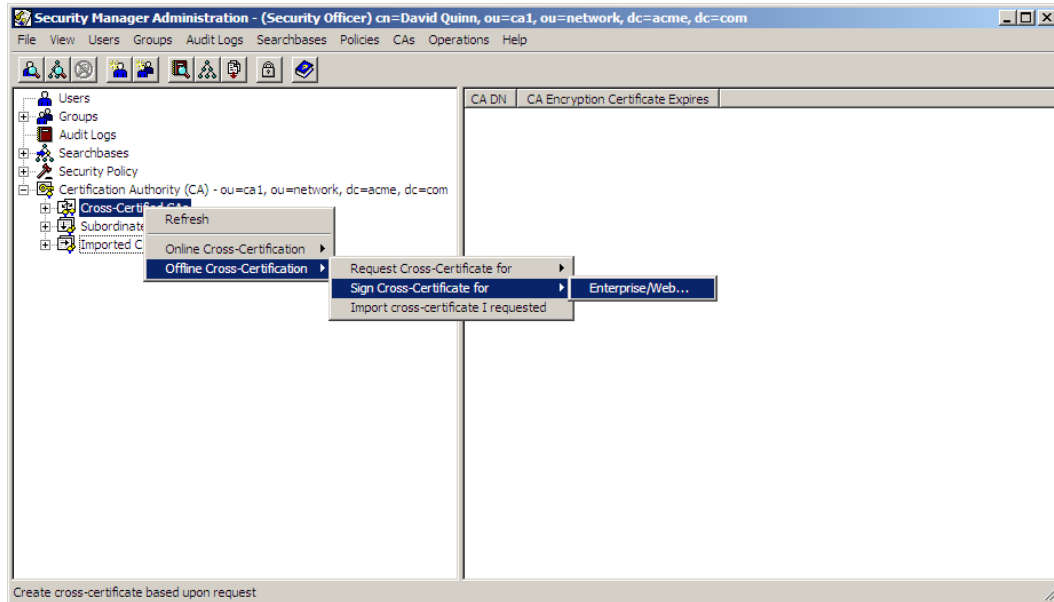


- After agreement with the other party CA Security Officer you would provide them with this file in a secured manner and in a different transmission provide the **Validation String** information.

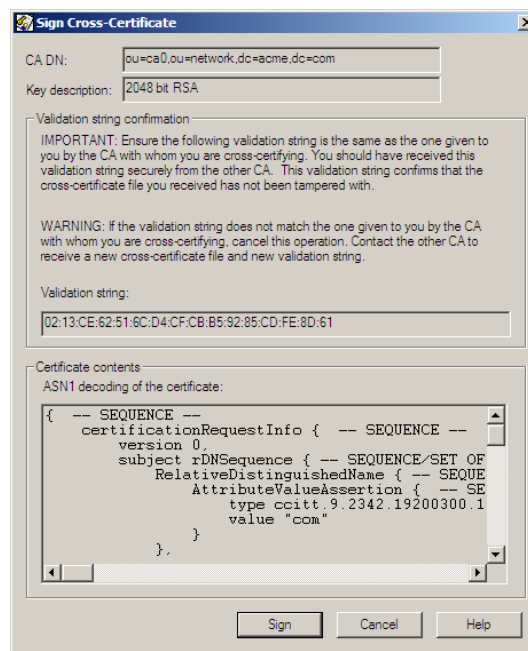
## Exercise 3: Complete an offline cross-certification

Each Security Officer will import the trust from other CA to cross certify. This is done by signing the request from the other CA.

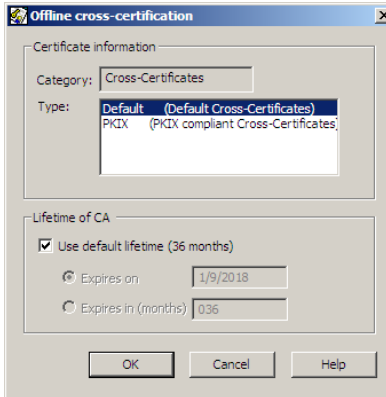
- 1 Log in Entrust Authority Security Manager Administration as a Security Officer.
- 2 In the left-hand pane, expand **Certification Authority** and right-click **Cross-Certified CAs**. Click **Offline Cross-Certification > Sign Cross-Certificate for > Enterprise/Web**.



- 3 Browse and locate the `student1.der` file provided in the Source folder classroom files and click **Open**. Also open the validation string file.
- 4 Review the information in the PKCS#10 request and verify the **Validation string** to ensure it matches with the one generated when the cross-certificate request was created. If the validation strings match, click **Sign**.



- 5 Select the **Type** of cross-certificate and the **Lifetime of CA** settings and click **OK**.



- 6 Authorize the activity by typing the Security Officer password.

The status of the cross-certification relationship should now be displayed in Entrust Authority Security Manager Administration as **Complete**.



**Note:**

You can also import the **Cross-Certificate I Requested** (that is, the forward cross-certificate) from any other cross-certified CA. The forward cross-certificate contains your Certification Authority verification key and is signed by the other Certification Authority. The process of importing the forward cross-certificate is similar to offline cross-certification, but completed in a reverse direction. The other Certification Authority would write the forward cross-certificate to a file, and deliver it securely to your Certification Authority. Your Certification Authority would then import the forward cross-certificate.

# Discussion Questions

- 1 An organization extends trust to users in another Certification Authority domain through cross-certification. The organization decides that their cross-certified partner is no longer maintaining their Certification Authority in a trustworthy manner and wish to terminate the relationship. How can this be performed in Entrust Authority Security Manager?
- 2 Can Entrust Authority Security Manager cross-certify with a Certification Authority from another vendor? If so, how? If not, why not?

## Hierarchical Cross Certification

This lab has no hands on components but continues the discussion from network cross certification in the previous lesson.

## Discussion Questions

- 1 Why would an organization choose to use hierarchical cross-certification instead of network cross-certification to extend trust to users in another Certification Authority domain?
- 2 An organization installs Entrust Authority Security Manager as a root Certification Authority. After a corporate restructuring, the organization attempts to move this Certification Authority to be subordinate to another. How can this operation be performed?

## CA Key Update

This lab has you use the utilities to identify the current CA signing key parameters, how to change them and perform a key update on hold.

## Lab

In these exercises, participants will prepare for and execute a CA key update

### Tasks

The following tasks will be completed:

1. New CA signing Key Algorithm and key length will be defined
2. New Extension will be added to Certificate definition
3. CA key will be generated for viewing using CA Certificate preview
4. New CA Key will be generated
5. Follow-up administration tasks will be discussed
6. Key update will be completed on a system

### Timing

Estimated time to complete these exercises is 45 minutes.

## Exercise 1: View current CA Signing Key Parameters

1. Login to the Master Shell as a Master User (i.e. Master1) and use the *ca cert* commands to view the current CA signing key details and note the current settings:

- *ca cert query*



```
Security Manager Control Command Shell
Entrust Authority (TM) Security Manager Control Command Shell 8.2.11(265)
Copyright 1994-2017 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
entsh$ login
Master User Name: Master1
Password:
You are logged in to Security Manager Control Command Shell.
ou=ca0,ou=network,dc=acme,dc=com.Master1 $ ca cert list
Serial Type Issue Date Expiry Date Post Revoked
[1] CA 2015/12/07 15:41:31 2025/12/07 16:11:31 yes

The certificate with serial number [1] is the current CA certificate.

Serial Numbers:
[1] 5665AFB3 (1449504691)

ou=ca0,ou=network,dc=acme,dc=com.Master1 $ ca cert query
CA certificate lifetime (in months) 120
CA private key usage (% of CA certificate lifetime) 100.0000

ou=ca0,ou=network,dc=acme,dc=com.Master1 $ _
```

2. Perform a full backup.

- *db backup full*

## Exercise 2: Identify new Algorithm, key length and lifetime for next CA keys and Certificates

1. Using the *ca key* and *ca cert* commands identify the current key length, algorithm and expiry used.



```
Security Manager Control Command Shell

ou=ca0,ou=network,dc=acme,dc=com.Master1 $ ca key config query
keyType = RSA-2048
signatureAlg = RSA-SHA256
parameters = [none]
ou=ca0,ou=network,dc=acme,dc=com.Master1 $ _
```

2. Using the *ca key config help*, identify and execute a command to change the key length and algorithm to your liking.

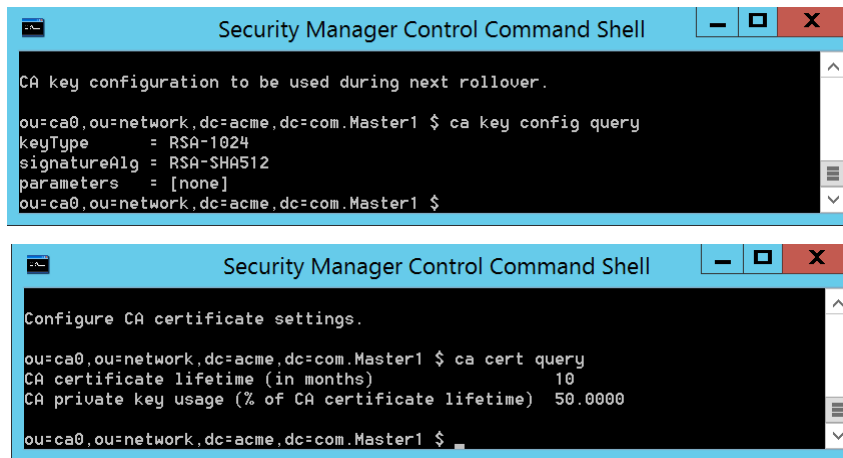
3. Using the *ca cert config help*, identify and execute a command to change the CA verification certificate lifetime and settings to your liking.

- *ca key config -keytype*                      *-signatureAlg*
- *ca cert config -lifetime*                      *-period*

## Exercise 3: Check updated config

1. Using the `ca` commands, list the settings for the next CA keys and certificate and verify your changed settings.

- `ca key config query`
- `ca cert query`



```
Security Manager Control Command Shell
CA key configuration to be used during next rollover.
ou=ca0,ou=network,dc=acme,dc=com.Master1 $ ca key config query
keyType = RSA-1024
signatureAlg = RSA-SHA512
parameters = [none]
ou=ca0,ou=network,dc=acme,dc=com.Master1 $

Security Manager Control Command Shell
Configure CA certificate settings.
ou=ca0,ou=network,dc=acme,dc=com.Master1 $ ca cert query
CA certificate lifetime (in months) 10
CA private key usage (% of CA certificate lifetime) 50.0000
ou=ca0,ou=network,dc=acme,dc=com.Master1 $
```

## Exercise 4: Perform a key update and hold on the CA keys

- 1 Perform a *CA key update on hold* which will create not only the CA cert but the link certificates and new root key. They will not be active yet, but you will be able to view all of the certificates that will be created.

- `ca key update -hold`



```
Security Manager Control Command Shell

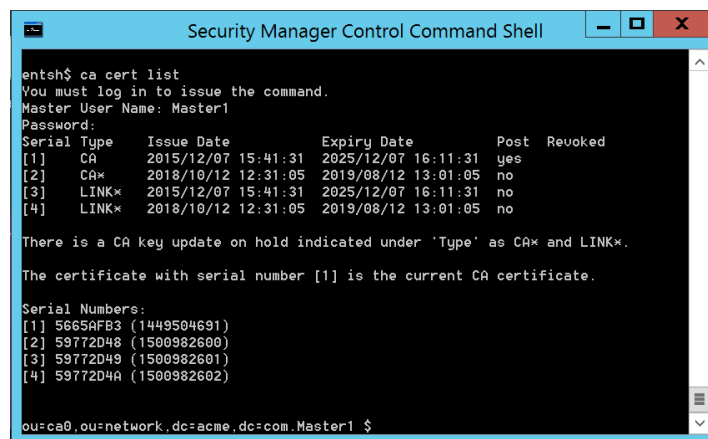
entsh$ ca key update -hold
You must log in to issue the command.
Master User Name: Master1
Password:

Select the destination for the new CA key.
Choose one of:
1. Software
2. Cancel operation
> 1
100% complete. Estimated time remaining -:-- \

CA key and certificate successfully updated and are on hold (not active).
The CA key update may be completed or canceled at a later date using the
'ca key update' command.
ou=ca0,ou=network,dc=acme,dc=com.Master1 $
```

- 2 Using the `ca` commands, list the settings for the next CA keys and certificate and verify your changed settings.

- `ca cert list`



```
Security Manager Control Command Shell

entsh$ ca cert list
You must log in to issue the command.
Master User Name: Master1
Password:

Serial Type Issue Date Expiry Date Post Revoked
[1] CA 2015/12/07 15:41:31 2025/12/07 16:11:31 yes
[2] CA* 2018/10/12 12:31:05 2019/08/12 13:01:05 no
[3] LINK* 2015/12/07 15:41:31 2025/12/07 16:11:31 no
[4] LINK* 2018/10/12 12:31:05 2019/08/12 13:01:05 no

There is a CA key update on hold indicated under 'Type' as CA* and LINK*.

The certificate with serial number [1] is the current CA certificate.

Serial Numbers:
[1] 5665AFB3 (1449504691)
[2] 59772D48 (1500982600)
[3] 59772D49 (1500982601)
[4] 59772D4A (1500982602)

ou=ca0,ou=network,dc=acme,dc=com.Master1 $
```

## Exercise 5: Administration Planning prior to key update

1. Now that you have your CA ready for a key update, review the administration activities that will be required in support of this CA key update.

Consider the following user / certificate recipients:

- Users of Entelligence or other plug-ins
- End users with custom applications based on API
- End users using browser certificates
- Devices using SSL certificates
- Devices issued smart credentials
- Cross Certified CAs
- CAs above this CA in Hierarchy
- Subordinate CAs

## Exercise 6: Perform Key Update

1. On one of the systems, perform the key update.
  - ca key update -complete
2. Accept any prompts to issue new CRL.
3. Once the key update is complete, complete a full backup
  - db backup full
4. Once the backup is finished, restart the services and login to Administration as the First Officer.

## Disaster recovery

In this lab you will prepare for and simulate a disaster for a Security Manager Installation that is using the provided PostGres Database.

## Lab

In these exercises, participants will backup their Certificate Authority and then restore after a simulated disaster.

### Tasks

The following tasks will be completed:

Exercise 1: Stop the services

Exercise 2: Copying of authdata folder

Exercise 3: Uninstall your CA and Database

Exercise 4: Restore Entrust Authority Security Manager Database

Exercise 5: Refresh content in the Directory

### Timing

Estimated time to complete these exercises is 25 minutes

## Exercise 1: Stop the services

In this exercise, all Entrust Authority Security Manager-related services will be stopped.

- 1 Perform a full backup for your PKI.
- 2 Log into Entrust Authority Security Manager Control Command Shell as a Master User and enter the following command to stop the Entrust Authority Security Manager services and subsystems:

```
service stop
```

After the services have stopped, exit the Entrust Authority Security Manager Control Command Shell.

- 3 Open Windows Services and stop the Entrust PostgreSQL Database service.
- 4 Close any open Entrust Authority Security Manager Administration windows and ensure that no users are logged into their security stores through Entrust Entelligence Security Provider.

## Exercise 2: Copying of authdata folder

- 1 Simulate that your OS has backed up the authdata folder by copying your *authdata* folder and renaming to *authdata.old*.



**Note:**

In the class the authdata folder already exists, but outside of the class this folder will need to be copied from your manual backup of the /authdata folder. The files that are required are the /archive, /logs and /manager/epf for any local profiles for this CA. In production these will normally be on different systems from the CA.

---

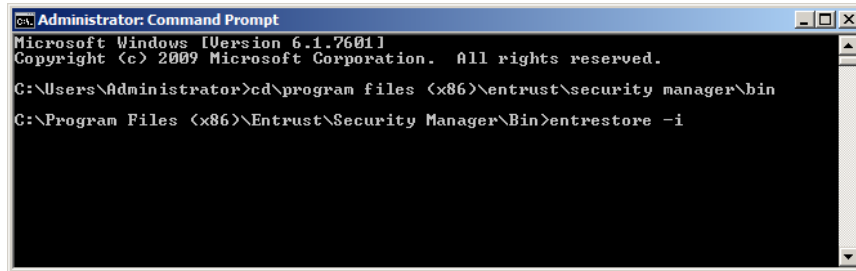
### Exercise 3: Uninstall your CA and Database

- 1 Using the Control Panel, uninstall Entrust Security Manager
- 2 Using the PostGres Installer (source directory) uninstall the Entrust PostGres Database.
- 3 Navigate to C:\Program Files\Entrust and delete the Security Manager folder. This will clean out any additional files left by the uninstaller.
- 4 **Reboot** your machine. (DO NOT shutdown)
- 5 Login to your machine.
- 6 Reinstall the PostGres Database using the same parameters (passwords, ports etc) as the original installation.
- 7 Reinstall the Entrust Security Manager.
- 8 Using Services, **stop** the new Entrust PostGres Database service.

## Exercise 4: Restore Entrust Authority Security Manager Database

In this exercise, the database backup will be restored.

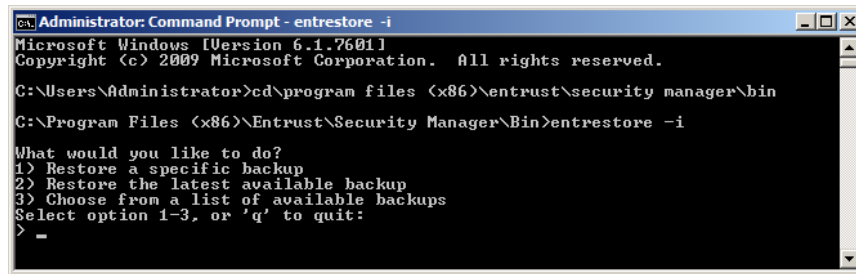
- 1 Open a DOS Command Prompt.
- 2 Navigate to the following folder:  
C:\Program Files\Entrust\Security Manager\bin
- 3 Type the following command:  
entrestore -i



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\program files <x86>\entrust\security manager\bin
C:\Program Files <x86>\Entrust\Security Manager\Bin>entrestore -i
```

- 4 When prompted, select **3) Choose from a list of available backups.**

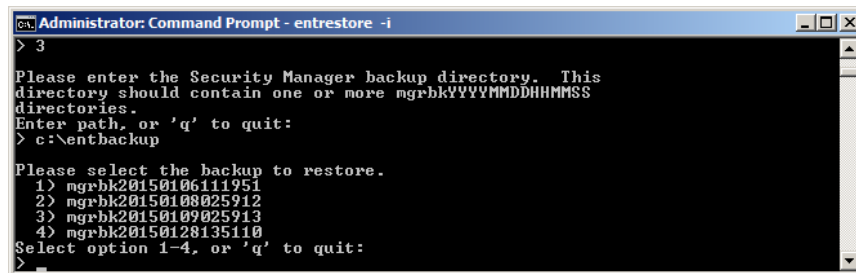


```
Administrator: Command Prompt - entrestore -i
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\program files <x86>\entrust\security manager\bin
C:\Program Files <x86>\Entrust\Security Manager\Bin>entrestore -i

What would you like to do?
1) Restore a specific backup
2) Restore the latest available backup
3) Choose from a list of available backups
Select option 1-3, or 'q' to quit:
> 3
```

- 5 Type the path of the backup folder, for example, C:\entbackup.
- 6 A list of available backups will be displayed, type the number of the backup selected in Exercise 2 above.



```
Administrator: Command Prompt - entrestore -i
> 3

Please enter the Security Manager backup directory. This
directory should contain one or more mgrbkYYYYMMDDHHMMSS
directories.
Enter path, or 'q' to quit:
> c:\entbackup

Please select the backup to restore.
1) mgrbk20150106111951
2) mgrbk20150108025912
3) mgrbk20150109025913
4) mgrbk20150128135110
Select option 1-4, or 'q' to quit:
> 1
```

- 7 Select **1) Full restore.**

- 8 When prompted about the integrity of the Write Ahead Log (WAL) files, type `n` for no.

```
Administrator: Command Prompt - entrestore -i
C:\> mgrbk20150128135110
Select option 1-4, or 'q' to quit:
> 3

Selected backup: c:\entbackup\mgrbk20150109025913

What type of restore would you like to perform?
1) Full restore.
2) Point-in-time recovery.
Select option 1-2, or 'q' to quit:
> 1

Is the database walfile directory intact?
Enter y/yes, n/no, or 'q' to quit:
> n
```

- 9 The database is restored.

```
Administrator: Command Prompt - entrestore -i
Restoring full backup 'c:\entbackup\mgrbk20150128135110\Database'.
Removing database datafile directory 'C:\easm_entrust_pg_data'.
Restoring database datafiles from 'c:\entbackup\mgrbk20150128135110\Database\pgbkup.zip' to 'C:\'.
Salvage was not requested. Removing 'C:\easm_entrust_pg_tx_logs'.
Recreating walfile directory 'C:\easm_entrust_pg_tx_logs'.
Removing file 'C:\easm_entrust_pg_data\postmaster.pid' before restarting PostgreSQL.
Starting the database to perform recovery.
SUCCESS: Database restore completed successfully.

WARNING***: Run a full backup as soon as you are satisfied that you are operational.

WARNING***: Incremental backups will be unusable until such a full backup has been run.

Reminder:
Before bringing Security Manager online, you must resynchronize your serial numbering scheme.
Please run the entsh command 'ca resynch-next-cert-serial'
```

- 10 Verify that the PostGres Database is running.
- 11 Create a folder `C:\authdata` and copy the files from your backup in `c:\entbackup\<filename>`. These files are the minimum files required to restore your CA. The additional files will be retrieved from the database now that the database is now restored.
- 12 Open the Security Manager Command Shell, and enter the command  
`node join -bootstrapdir "c:/authdata/bootstrap" -authdatadir "c:/authdata"`



**Note:**

In production this command looks like `node join -bootstrapdir <bootstrap directory location> -authdatadir <authdata directory location>`

- 13 If passwords for the Database are correct, you will now be prompted to login to the Master Shell as a Master User to complete the restore.



- 14 At this point, the restore has completed and you will have a working CA, however at this point it is a good idea to restore the additional files mentioned earlier that were backed up by the OS. (/archive,/logs and /manager/epf). **Ensure you do not replace the CA.epf file in the /manager/epf folder.**



**Note:**

In the classroom these files can be retrieved from the folder you renamed **authdata.old**

---

## Exercise 5: Refresh content in the Directory

In this exercise, serial numbers for certificates will be resynched and Directory content will be brought up to date.

- 1 Still logged into Entrust Authority Security Manager Control Command Shell, type the following command to resynch the certificate serial number counter:

```
ca resynch-next-cert-serial
```

- 2 Type the following command to refresh all the certificates in the Directory:

```
dsa restore all
```

- 3 Type the following command to refresh all the revocation lists in the Directory:

```
rl issue -all
```

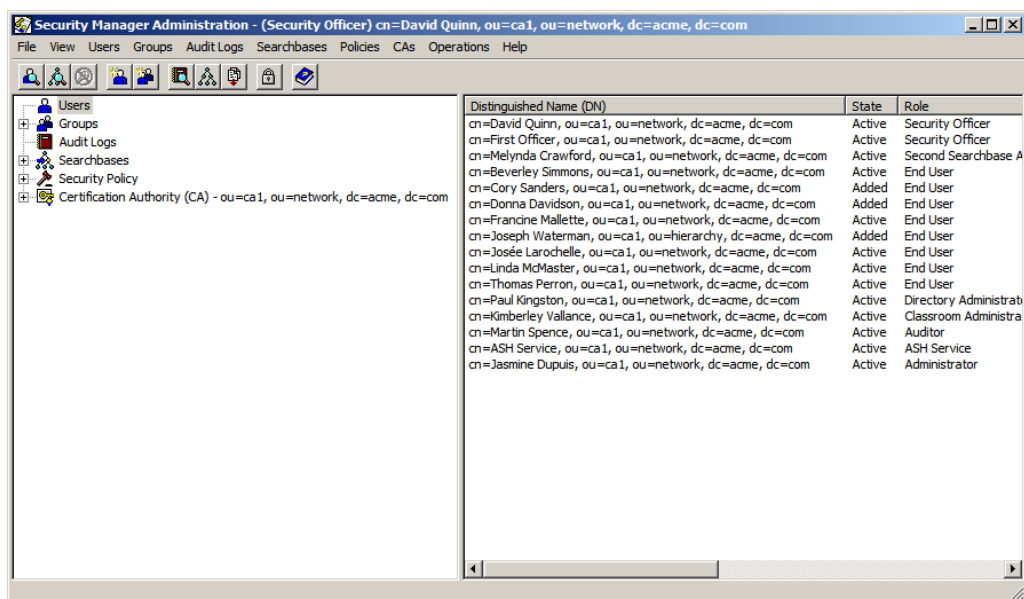
- 4 Start the Services.

```
service start
```

- 5 Log out of the Entrust Authority Security Manager Control Command Shell.

- 6 Log into Entrust Authority Security Manager Administration as a Security Officer.

- 7 Verify that the systems is back to the state before the cross-certification exercise.





## Entrust Authority Administration Services

This lab will introduce you to Admin Services and the UMS (User Management System) and URS (User Registration Service) interfaces. UMS is the recommended user management interface for device and end user account management.

## Lab

In these exercises, you will activate your MPKI trial and login as an administrative user to manage accounts.

## Tasks

The following tasks will be completed:

- Complete activation of Administrative user in UMS and follow evaluation guide for exercises
- Complete the exercises from the Evaluation guide

## Timing

Estimated time to complete these exercises is 60 minutes

## Complete activation of Administrative user in UMS and follow evaluation guide for exercises

In this exercise, the UMS Admin PKCS#12 file will be created and imported into Chrome or IE.

- 1 In your welcome email from the MPKI trial record the configuration identifier, Reference Number and Authorization code

### Welcome to Entrust Datacard mPKI!

Your evaluation trial for sst0825 has started, please use the codes below to enroll your RA credential.

**Reference Number:** 02440797

**Authorization Code:** VWZM-QONO-EFJG

These codes will expire in 14 days. You can enroll a p12 credential using the [User Registration Service](#).

Your configuration identifier will be: sst082\_user

Click on "Generate My Digital ID" and enter the codes above to create your **Registration Authority p12 profile**.

Your evaluation period will end on 2020-10-24.

### Get Started!

Here are some ways you can leverage your mPKI evaluation environment:

- 2 Also download the Evaluation guide from the link at the bottom of the email.

**V8 URL:** <https://apitest.managed.entrust.com/mdmws/services/AdminServiceV8>

**V9 URL:** <https://apitest.managed.entrust.com/mdmws/services/AdminServiceV9>

**V11 URL:** <https://apitest.managed.entrust.com/mdmws/services/AdminServiceV11>

**MDM-SCEP URL:** <https://apitest.managed.entrust.com/scep>

**Username:** sst102mdmadmin

**Password:** sst102Ev@luat3

**Managed CA Name:** mPKI Evaluation Issuing CA

**Digital ID Name:** sst102 Mobile ID

**DN Format:** cn=<igusername> <iggroup> <devicetype>

For more information and assistance please refer to the [mPKI Evaluation Quickstart Guide](#) or contact an Entrust Datacard mPKI representative.

- 3 Proceed through the instructions in the email to activate your account.
- 4 Then proceed through the evaluation guide to perform some operations in Administration Services User Management Service that you have already done in the Administration tool
- 5 Note the similarities and differences from Administration to Administration Services.

