

Installing and configuring the Entrust Certificate Services application

Document issue: 1.0

Date of issue: January 2019



Copyright © 2019 Entrust Datacard. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust Datacard Limited in Canada. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. or Entrust Datacard Limited 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 Datacard 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.

Contents

Contents	3
Revision, audience and guide information	4
<i>Revisions</i>	4
<i>Audience</i>	4
<i>Viewing this guide</i>	4
<i>Conventions</i>	4
Introduction	5
<i>Overview of the installation</i>	5
Before you begin	5
Installing the Entrust application	5
To install the application	5
Configuration	6
<i>Uploading the API administrator key store and configuring the Protocol Profile</i>	6
<i>Configuring the basic authentication profile</i>	9
<i>Testing the configuration</i>	11
Create Certificate Services user groups and assign users	12
To create user groups	12
To assign users to Certificate Services roles	14
Initialize the database	16
Appendix A: Creating a web service client profile	18
To create a Public/Private key pair stored in a Java JKS	18
<i>Use Entrust Certificate Services Enterprise to create an SSL certificate</i>	19
<i>Create a new API user</i>	21

Revision, audience and guide information

Revisions

Revision	Section	Description
January 2019	n/a	Initial release of document.

Audience

This guide is intended for administrators who want to use their ServiceNow account to create and manage Entrust Certificates. Procedures assume that the persons installing and configuring the application are knowledgeable ServiceNow administrators.

Viewing this guide

This guide contains hyperlinks between sections. It is intended to be used in PDF format.

Conventions

In places, this guide uses ECS or Certificate Services to refer to Entrust Certificate Services.

In places, this guide uses “the API” or “ECS API” or “ECS SOAP API” to refer to the Entrust Certificate Services web service.

Introduction

The Entrust Certificate Services (ECS) application is used to obtain and manage certificates. Users require an Entrust Certificate Services Enterprise pooling account to create or renew certificates from ServiceNow.

Overview of the installation

Note: To use the Certificate Services web service to create and manage certificates, you must have an Entrust Certificate Services Enterprise pooling account. For information about obtaining an Entrust Certificate Services Enterprise account click [here](#).

1. From your Certificate Services Enterprise pooling account, create a Certificate Services Web Service account to use with ServiceNow. If you do not know how to create this type of account, see [Appendix A: Creating an ECS client profile](#).
2. Install the Certificate Services application package from the ServiceNow app store.
3. Upload the key store (P12/pfx or Java jks formats only). To use the key store you must supply key store password. This key store is used to establish a secure connection with the API. You will also need to supply the basic authentication user name and password to provide access to the Certificate Services API account.
4. Create Certificate Services groups with specific user roles.
5. Assign users to the Certificate Services groups.
6. Initialize the database.
7. Obtain the User Guide from the ServiceNow App Store or by following [this link](#).

Note: This application depends on Service Management Core and State Flow plugins. Please contact your ServiceNow representative to determine if this will have licensing impacts for you.

Before you begin

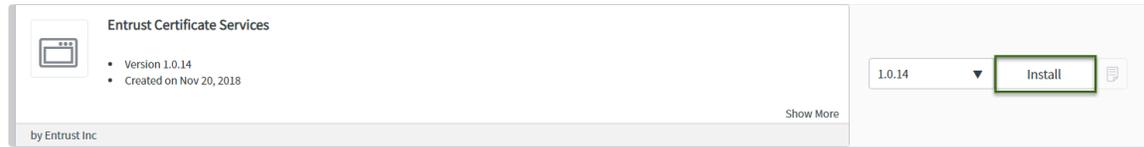
If you have not yet created the API administrator account and key store, do so before beginning the installation. Use either the P12/pfx or Java jks format. If you need information about creating a key store see the section: [Appendix A: Creating a web service client profile](#)

Installing the Entrust application

To install the application

1. Navigate to **System Applications > Search ServiceNow Store**.
2. Find and select **Entrust Certificate Services**.
3. Click **Install**.

Not Installed



- A progress bar appears. A success/failure message appears when the installation is completed. If the installation is successful, Entrust Certificate Services appears in the Application Manager page under “Installed” applications.

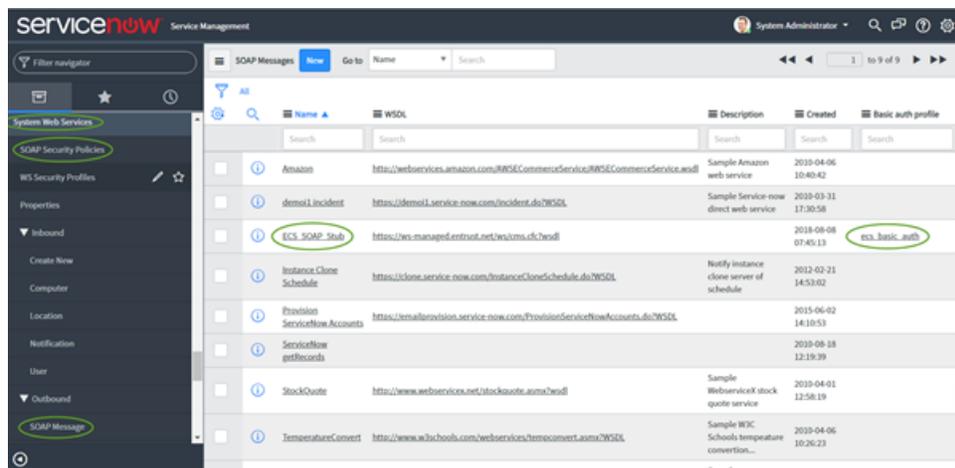
Configuration

After the Application is installed, you must configure a secure connection to the Entrust Certificate Services Enterprise API. To do this you need to create an API administrator account, upload the key store that the account uses to ServiceNow, and provide the appropriate authentication. This allows ServiceNow to use the Entrust Enterprise API to create and manage certificates.

Uploading the API administrator key store and configuring the Protocol Profile

When you have the Entrust Certificate Services API key store, proceed with the following steps:

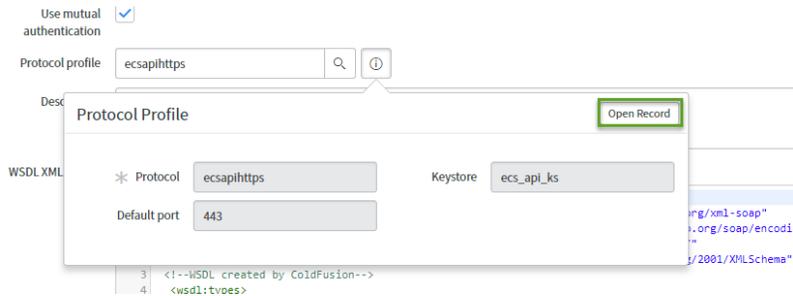
1. Find the Entrust application in the menu. Navigate to **System Web Services > Outbound > SOAP Message > ECS SOAP Stub**



2. In the notification message at the top of the page, click **here** in **To edit this record click here**.
3. Click information (i) to the right of the **Protocol profile** field.



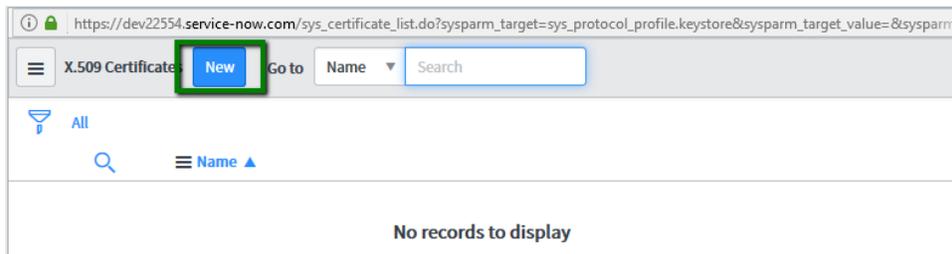
4. On the Protocol Profile configuration page, click **Open Record**.



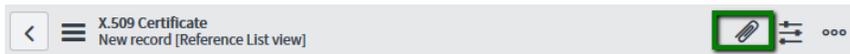
5. In the Protocol Profile page click details (🔍).



6. On the **X.509 Certificate** page, click **New** to update the ECS SOAP API key store.



7. On the next page, click attach (📎) to attach a valid API credential from Entrust. The credential must be in either P12/pfx or Java jks format.



8. In the popup, click **Browse** and navigate to the location of the key store. Select and load the key store file.

Attachments



9. When the key store file is attached, close the dialog box.

Attachments



No files selected.

[snapiuser.jks](#) [rename] [view]

10. Enter the name of the key store and select the key store type. **Java Key Store** is used here as an example.

Manage Attachments (1): [snapiuser.jks](#) [rename] [view]

<p>* Name</p> <input type="text"/>	<p>Format</p> <input type="text" value="PEM"/>
<p>Expiration notification</p> <input type="checkbox"/>	<p>Type</p> <input type="text" value="Trust Store Cert"/>
<p>Active</p> <input checked="" type="checkbox"/>	<p>Trust Store Cert</p> <p>Java Key Store</p> <p>PKCS12 Key Store</p> <p>Private Key</p>

11. Enter the password of the key store and click **Validate Store/Certificates**.

Manage Attachments (1): [snapiuser.jks](#) [rename] [view]

<p>* Name</p> <input type="text" value="ecs_api_ks"/>	<p>Type</p> <input type="text" value="Java Key Store"/>
<p>Active</p> <input checked="" type="checkbox"/>	<p>Key store password</p> <input type="password" value="....."/>
<p>Short description</p> <input type="text"/>	
<input type="button" value="Update"/>	<input type="button" value="Delete"/>

Related Links

[Validate Stores/Certificates](#)

12. When the key store is validated, click **Update** to continue.

Valid key_store [X]

Manage Attachments (1): snapiuser.jks [rename] [view]

* Name: Type:

Active: Key store password:

Short description:

Update Delete

Related Links
[Validate Stores/Certificates](#)

13. On the X.509 Certificate page, select the key store that you updated.

X.509 Certificates **New** Go to

All

Name ▲

ecs api ks

14. The Protocol profile page displays the key store. Click **Update** to save your changes.

Protocol Profile
 ecsapihttps **Update** **Delete**

Defines an association between a unique protocol and a keystore and default port. [More Info](#)

* Protocol: Keystore:

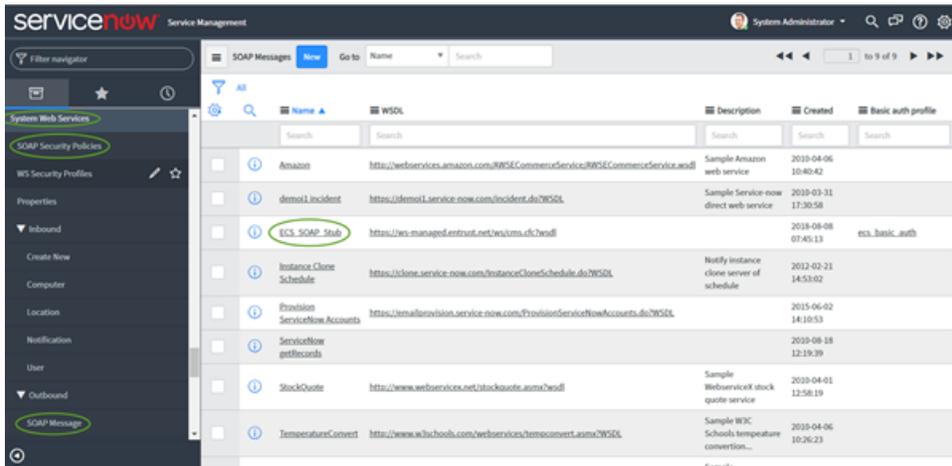
Default port:

Update Delete

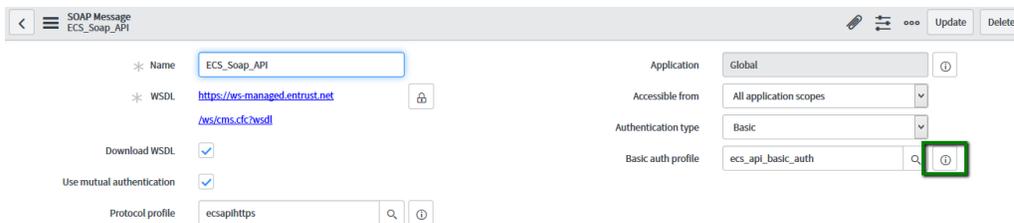
Next, configure the basic authentication profile as outlined in the following procedure.

Configuring the basic authentication profile

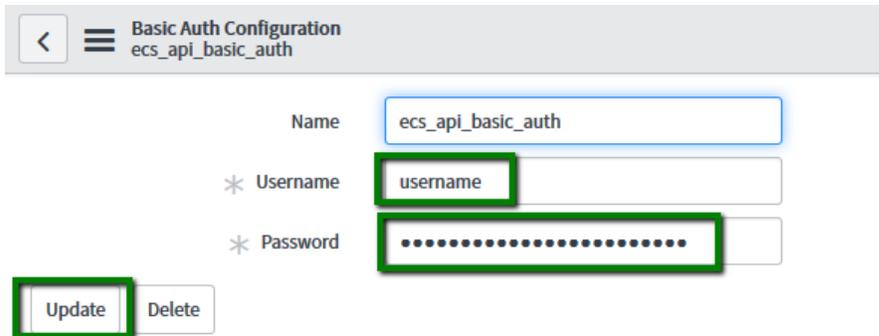
1. Find the Entrust application in the menu. Navigate to **System Web Services > SOAP Security Policies > Outbound > SOAP Message > ECS SOAP Stub**



- On the ECS_SOAP_API page, click information (i), to the right of the **Basic auth profile** field.



- On the Basic Auth Configuration page, replace the default user name and password with the username and password for the Certificate Services account. Click **Update**.



- Return to the ECS_SOAP_API page (you can use the back button) and click **Update** to commit your changes. Test the connection to the API, as outlined in the next procedure.

SOAP Message
ECS_Soap_API

Name: ECS_Soap_API

WSDL: <https://ws.managed.entrust.net/ws/cms.cf?wsdl>

Download WSDL:

Use mutual authentication:

Protocol profile: ecsapihttps

Application: Global

Accessible from: All application scopes

Authentication type: Basic

Basic auth profile: ecs_api_basic_auth

Update Delete

Testing the configuration

Check that the configuration works as expected.

1. On the SOAP Messages page, click **ECS_Soap_Stub**.

Name	WSDL	Description	Created	Basic auth profile
Amazon	https://webservices.amazon.com/RWSECommerceService/RWSECommerceService.wsdl	Sample Amazon web service	2010-04-06 10:40:42	
demo11 Incident	https://demo11.service.now.com/Incident.do?WSDL	Sample Service-now direct web service	2010-03-31 17:30:58	
ECS_Soap_Stub	https://ws.managed.entrust.net/ws/cms.cf?wsdl		2018-08-08 07:45:13	ecs_basic_auth
Instance Clone Schedule	https://clone.service.now.com/InstanceCloneSchedule.do?WSDL	Notify instance clone server of schedule	2012-02-21 14:53:02	
Provision ServiceNow Accounts	https://emailprovision.service.now.com/ProvisionServiceNowAccounts.do?WSDL		2015-06-02 14:10:53	
Serviceflow getRecords			2010-08-18 12:19:39	
StockQuote	https://www.webservices.net/stockquote.asmx?wsdl	Sample WebServiceKit stock quote service	2010-04-01 12:58:19	
TemperatureConvert1	https://www.w3schools.com/webservices/temconvert.asmx?WSDL	Sample W3C Schools temperature conversion...	2010-04-06 10:26:23	

2. On the SOAP Message ECS_Soap_Stub page, scroll down to the bottom and click **getOrgList** in the message list.

<input type="checkbox"/>	restoreCert	<soapenv:Envelope xmlns:xsi="http://www....
<input type="checkbox"/>	getCertList	<soapenv:Envelope xmlns:xsi="http://www....
<input type="checkbox"/>	getOrgList	<soapenv:Envelope xmlns:xsi="http://www....

3. On the SOAP Message Function getOrgList page, click **Test**.

Envelope XML

```

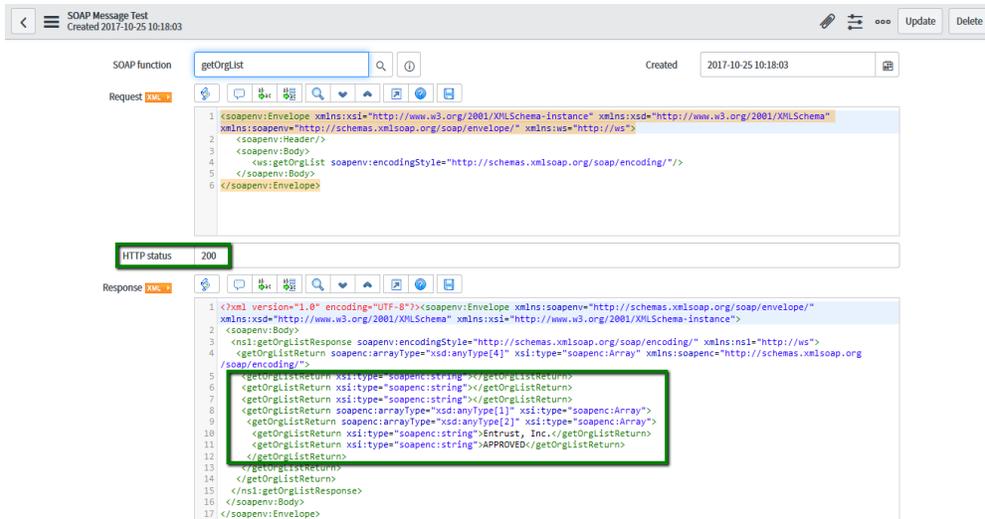
1 <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws">
2   <soapenv:Header/>
3   <soapenv:Body>
4     <ws:getOrgList soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" />
5   </soapenv:Body>
6 </soapenv:Envelope>

```

Update Delete

Related Links
[Auto-generate variables](#)
[Preview Script Usage](#)
[Refresh SOAP message](#)
[Test](#)

4. Check information on the next page. **HTTP Status** should be 200 and the response should not include any errors.



Create Certificate Services user groups and assign users

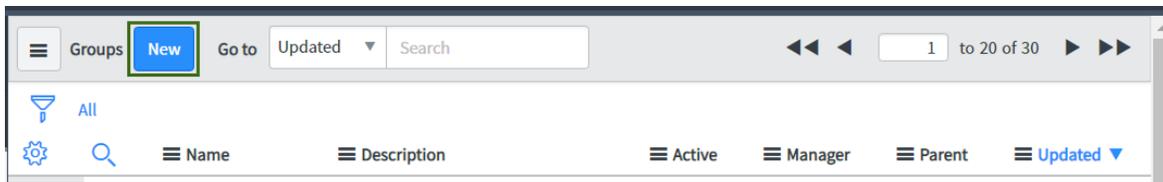
In this section, create groups for specific roles and assign users from your ServiceNow instance to the appropriate group. You can add or remove users from a group at a later date, as needed.

The Certificate Services application is designed to have the following two groups.

- Administrators have a full set of permissions. They can create, assign, and approve certificate requests as well as download and manage certificates.
- End Users have permission to create certificate requests and approve requests that are assigned to them.

To create user groups

1. Navigate to **System Security > Users and Groups > Groups**.
2. Click **New** to create a new group.



3. Enter a name for the group, group manager, and email address to receive notifications about the group. Add a meaningful description for the group.

Group
New record

Name: ECS_SSL_Admin

Group email: []

Manager: John Adams

Parent: []

Description: Administrator group for Entrust Certificate Services application.

Submit

4. Click **Submit**.
5. In the Groups page, add the roles associated with each group.
 - a. Click one of the groups that you created: this procedure uses the administrator group.

Groups New Go to Updated Search

All

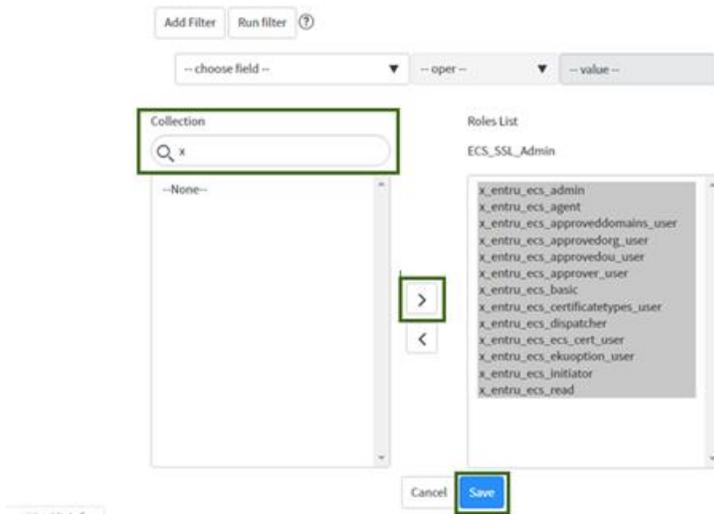
	Name	Description	Active
<input type="checkbox"/>	ECS_SSL_Admin		true
<input type="checkbox"/>	ECS_SSL_EndUser		true

- b. Click **Roles > Edit**.

Roles (13) Group Members (4) Groups

Roles Edit... Go to Created Search

- c. To find the Certificate Services roles, enter "x" in the **Collection** search field. For the administrator group, select all of the roles and use the arrow button to move them to the **Roles** List as shown below.



d. Click **Save**.

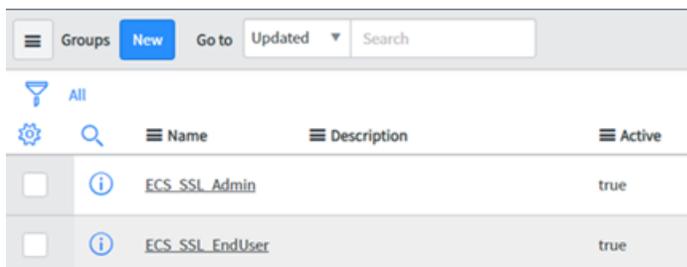
Repeat this procedure for the other group (in this case, the end user group). Give the end user group the following roles only.

- x_entru_ecs_basic
- x_entru_ecs_read
- x_entru_ecs_ecs_cert_user
- x_entru_ecs_ekuooption_user
- x_entru_ecs_approvedorg_user
- x_entru_ecs_approvedou_user
- x_entru_ecs_approveddomains_user

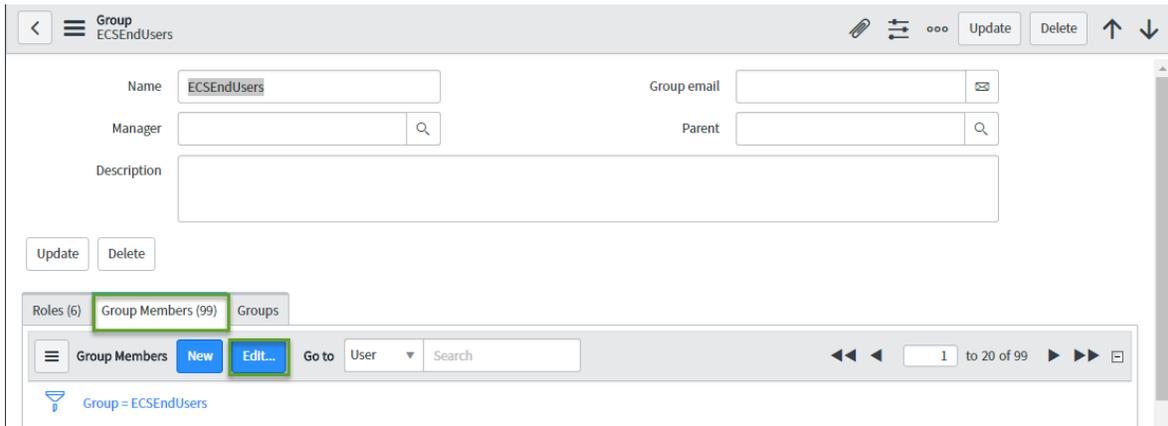
Assign users to your groups as outlined in the following procedure.

To assign users to Certificate Services roles

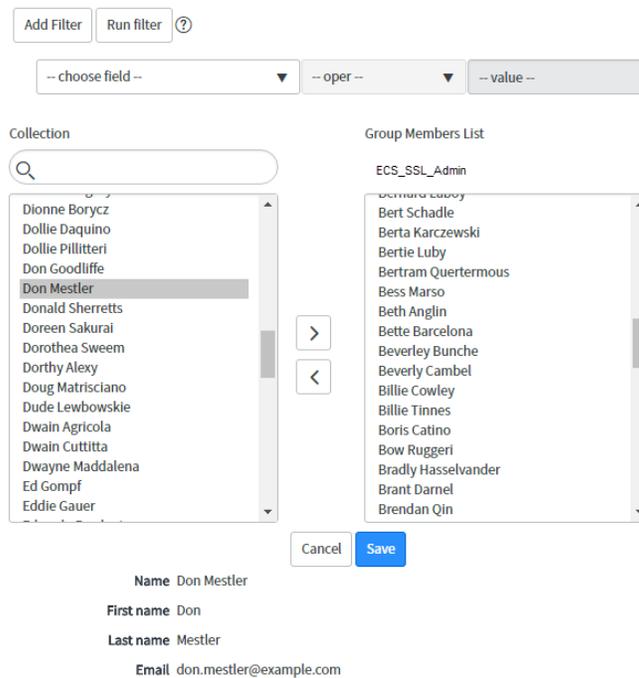
1. Navigate to **System Security > Users and Groups > Groups**.



2. Select the group that you want to configure.
3. Click **Group Members > Edit** to add users to the group.



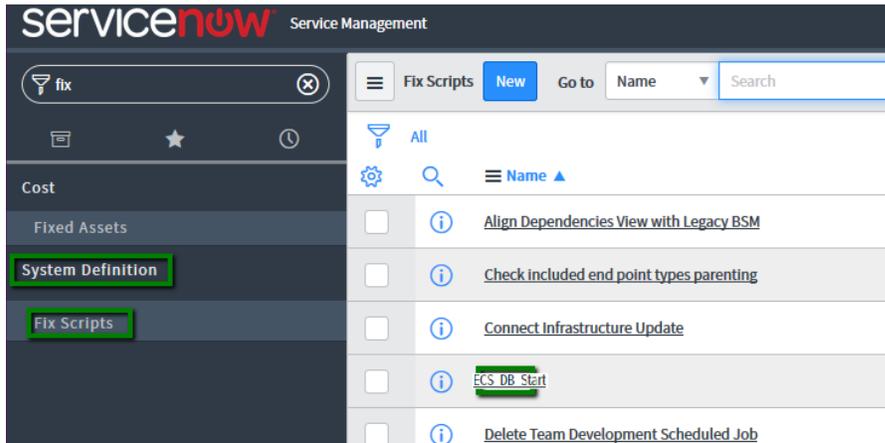
4. Select the users for this group and use the arrow button to move them to the **Group Members List**.



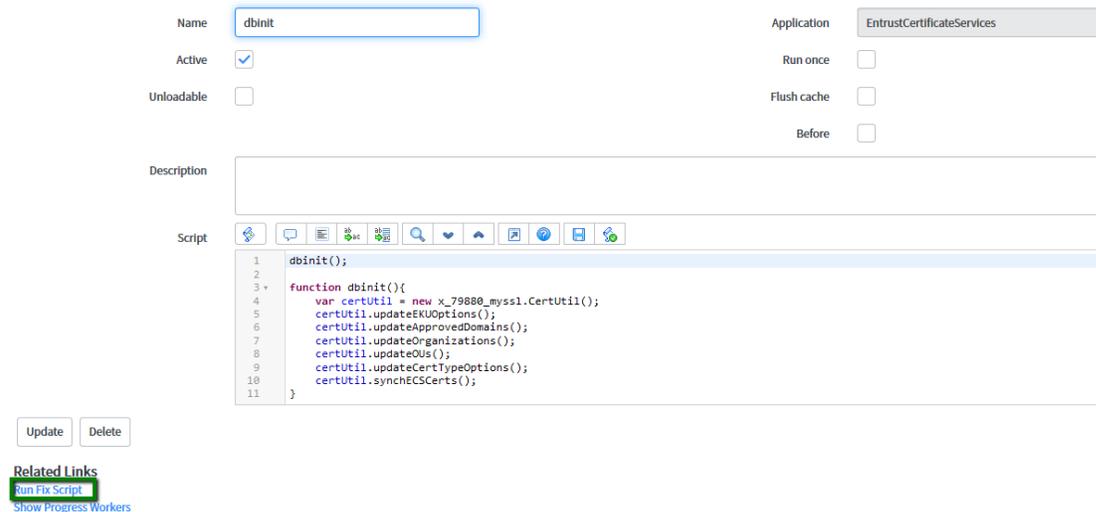
5. Repeat this procedure for the other Certificate Services group.
6. Click **Save**.

Initialize the database

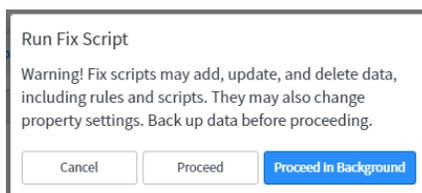
1. Navigate to **System Definition > Fix Scripts**. For example, search on **Fix Scripts**. Click **ECS_DB_Start** to initialize the application database records.



2. In the Fix Script dbinit page, click **Run Fix Script**.



3. A warning message appears. Click **Proceed**. Wait for the script to complete. This may take a minute or two.



4. Log out and close browser. Log in again.

This initializes the database and completes your installation. For information about using the Certificate Services application, see the *Entrust Certificate Services ServiceNow Application User Guide*.

Appendix A: Creating a web service client profile

The Certificate Services ServiceNow application must be able to authenticate to the Certificate Services web service API using SSL client authentication. To authenticate, the ServiceNow platform requires a key store in either PKCS12 or Java JKS format. The procedure below describes how to create a Java JKS key store for SSL client authentication.

Create the profile in the following stages:

1. Use keytool or a similar application to create a CSR (Certificate Signing Request).
2. In your Certificate Services account, create an SSL certificate with client authentication EKU (Extended Key Usage).
3. Create a web service super administrator with auto-approve. Enter the tracking ID in the tracking ID field for the SSL certificate that you just created. Record the user ID and password.
4. Download the certificate and its chain to the computer where you created the CSR. Use keytool to import the certificate and chain into the key store.
5. Import the key store into your ServiceNow instance when prompted during the update package installation.

To follow this example, you must have a working JDK installed on your computer. The example below uses OpenJDK version 1.8.0_118, however you can use any JDK including the Sun JDK version 6 or higher.

To create a Public/Private key pair stored in a Java JKS

1. Enter the following command from the folder where keytool is stored:

```
keystore ubuntu@ubuntu:~$ keytool -genkey -alias servicenow -keypass
servicenow keyalg RSA -keysize 2048 -keystore servicenow.jks -
storepass servicenow
```

2. Keytool will ask you to supply the information used to create the DN of the certificate.

```
what is your first and last name?
[Unknown]: servicenow.example.com
```

Replace example.com with the domain that you want to use. The domain must be verified before you can use it.

```
what is the name of your organizational unit?
[Unknown]: <organizational_unit>
```

This is an optional field. An example might be *Sales*.

```
what is the name of your organization?
[Unknown]: <your_organization>
```

Enter the name of your organization—for example, Example Inc.

```
what is the name of your City or Locality?
[Unknown]: <your_city>
```

Enter the name of your city—for example, Miami.

```
what is the name of your State or Province?
```

[Unknown]: <your_state>

Enter the name of your state or province—for example, Florida.

what is the two-letter country code for this unit?

[Unknown]: <country_code>

Enter the two letter country code—for example, CA or US.

3. You are prompted to check and accept or reject the DN formed from the information.

Is CN=servicenow.example.com, OU=Unknown, O=Example Inc., L=Miami, ST=Florida, C=US correct?

[no]: yes

4. Generate a Certificate Signing Request (CSR) using the following command.

```
ubuntu@ubuntu:~$ keytool -certreq -alias servicenow -keypass  
servicenow keystore servicenow.jks -storepass servicenow
```

Keytool generates the certificate request in Base64 format and displays it.

```
-----BEGIN NEW CERTIFICATE REQUEST----- encoded CSR data in Base64 format -----  
END NEW CERTIFICATE REQUEST-----
```

5. Copy all of the output from keytool including the "BEGIN NEW CERTIFICATE REQUEST" and "END NEW CERTIFICATE REQUEST" lines into a text file. You will use this CSR to request an SSL certificate from your Entrust Certificate Services Enterprise account.

Use Entrust Certificate Services Enterprise to create an SSL certificate

Create the web service API identity that the Certificate Services ServiceNow application uses to authenticate to the web service API.

1. Login to the Entrust Certificate Services portal. Select **Create > SSL/TLS**.
2. Select an SSL certificate type (Standard, for example).

The screenshot shows the Entrust Certificate Services portal interface. At the top, there is a navigation bar with 'Dashboards', 'Create', 'Certificates', 'Sites', 'Reports', 'Administration', and 'Help'. The 'Create' menu is open, showing options like 'SSL/TLS', 'Device', 'Code Signing', 'Secure Email Enterprise', 'Document Signing', 'Import Certificates', and 'Import Discovery Agent Scan Results'. The 'SSL/TLS' option is selected, and a sub-menu is visible with radio buttons for 'Advantage', 'EV Multi-Domain', 'UC Multi-Domain', and 'Wildcard'. The 'Standard SSL' option is selected. Below the menu, there is a progress bar with four steps: 'CERTIFICATE DETAILS', 'DOMAINS', 'OPTIONS', and 'ADDITIONAL INFORMATION'. The 'Standard SSL' section is highlighted, showing a description: 'The Standard SSL certificate establishes your trusted identity and eliminates browser notifications that warn visitors entering your site.' It lists features: 'Organization Validation (OV) SSL', 'Secures both www.example.com and example.com', and 'Includes Basic Website Security, by SiteLock'. A note at the bottom says: 'For greater trust and a green address bar, choose EV Multi-Domain SSL.'

3. Click **Next**.

4. Fill in the following fields:

- Certificate Expiry: Select the desired expiry date.

Note: If the certificate expires, the Certificate Services ServiceNow application will no longer be able to access the Certificate Services Enterprise API.

- **Organization:** Select an organization from the drop down list.
- **Extended Key Usage:** Select an EKU with Client Authentication.
- **Certificate Signing Request (CSR):** Paste the contents of the Certificate Signing Request obtained from the [previous procedure](#) into the field provided.

✓ Create Standard Certificate
New DN: cn=12345.example.com, o=Client2, l=Anytown, st=Ontario, c=CA

Certificate Expiry *
Jul 4, 2019

Organization *
TestClient

Organizational Unit
[no OU]

Signing Algorithm *
SHA2

Extended Key Usage *
Client Authentication

Send to CT logs

ⓘ This certificate will be sent to CT logs. The contents of this certificate, including host names, will be publicly visible

Use Entrust Turbo

Certificate Signing Request (CSR) *
BgNVBACTBk90dGF3YTELMAKGA1UECBMCT04xGjA9BgNVBAMTETETeYmZQ1LmV4YW1w bGUuY29tMlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEawUNz9tLeyx37 HQUoGv71/3gmH6SAqUifGSH2KZLiIKQYkWEExw5pnW5sSezcFvPmOoQpJUCYUr rkLKC9mq7SUOqo+sXKL+Uy4aMmmzryx0+0Zv8SmhzV3QpqrW+DHEco0WB9ZT8y1X sDtnEx5QUmPwjsCL1JzsrWEMVuM5Cu7HycdMOUHWfHjWq5r1m52xtusicYv2CKS 49Kh5GBbvWiaJNpF+LDtyh8y2DeC6/Lz5znBdlobNpvWisb4idV51WGaj01OXGs Nn1Ql4sXB2Z2pj/onfyYdgmDwAJmr3TEbcL GqrLHmrlZyWi94Ezz/TNpA4U+ZRmF g3aQ5H2GwiDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI2FgARzm+U5XJm9gRmj uTmLueW8fv0IXGx+D51lWRcEKmu+8xk64AkGK9F8PBFklnK+SbQ+yrw2CSEPD 0OZ6nohh0eEW08vRn0ndiqJB7OBW6drL0ukRLbEChikYnimlEbJRJTnkEKkCyfV qOHdNCi80Dga4QWCoTZzhQgbOFmWq0t0xH0SQPDQjYcVYC1G9K0IYC4IV/9zxHD QL+eJtnqw7McSCxNaaNGGLJT5qrm5L+elmKdjNnk2bFBHzoTSnkg8rtgn28hDSY8 rRVv5hYhgLmwmnnc5jpv1NdrS/YBnbHWBPqAh3RMK5S6TUZyVQc1HwwNeLkf+VZ 4UE= -----END CERTIFICATE REQUEST-----

[View CSR Details](#) [CSR Help](#)

5. Click **Next**.

6. Page through the certificate creation pages, entering any value you may want to use. For example you may want to identify the user as "ServiceNow" in the **Tracking info** field.

7. Click on **Yes** to create the client SSL certificate. You can pick up the certificate at this point by clicking the link or after you create the new API user. Details of how to acquire you certificate are available at the end of the next procedure.

- Your new certificate should appear at the top of the list of ECS Certificates. Record the Tracking ID of this certificate for use in the next section.

Tracking ID	Certificate Type	Common Name	Serial Number (Hex)	Pickup Status	SAN List	Organization (O)
268467	Standard	servicenow testcertificat...	AB9AFE69F819D646000000...	Ready	servicenow testc...	Entrust
267799	Standard	a11723161342.entrust.c...	AC31D976223C2A18000000...	Ready	a11723161342.e...	Entrust
264420	Document Signing Indivi...	Bruce Bateman	5CEBB2D000490480000000...	Active		Entrust
263584	Document Signing Indivi...	Bruce Bateman	.8C26C82E356D8275000000...	Active		Entrust
261172	Wildcard SSL	a116333133517.testcerti...	CBD2BCD32BC6D0DF0000...	Active	a116333133517.L...	Entrust
260870	Standard	a1173142743.testcertific...	14B24D44A7DC402F000000...	Suspended	a1173142743.les...	Entrust

Create a new API user

This is the identity that the Certificate Services ServiceNow application uses to authenticate to the Certificate Services web service.

1. From the menu options within the ECS portal, select **Administration > Advanced settings > API**.
2. In the **Add API Key** panel, click **Select a certificate**.

Add API Key

i Create a new API key. Many of the functions performed in the Entrust Certificate Services Portal can also be performed through the API.
 Click [here](#) to download the REST API for ECS Enterprise User Guide and Method Reference.
 Click [here](#) to download the REST API for ECS Enterprise API OpenAPI 2.0 Specification.
 Click [here](#) to download the Certificate Services Web Services Guide (SOAP API).

Step 1 **Select a certificate**

Step 2 **Generate credentials**

A list of certificates with client authorization opens.

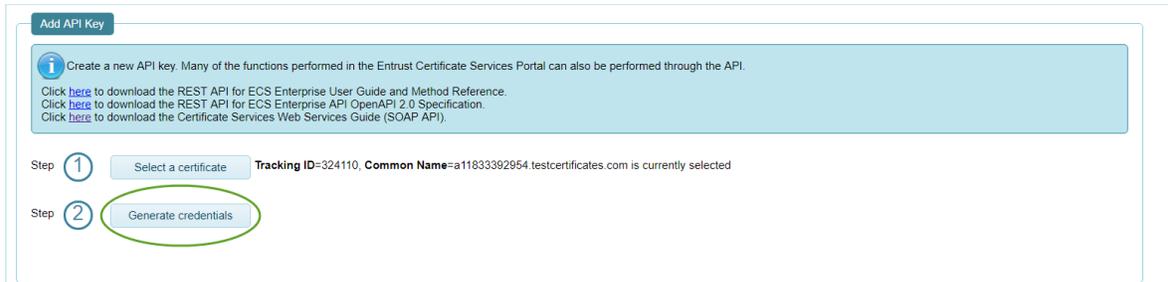
3. Scroll to the certificate that you created for this API account. Click **Choose this certificate**.

i Only Certificates that can be used for API authentication are shown

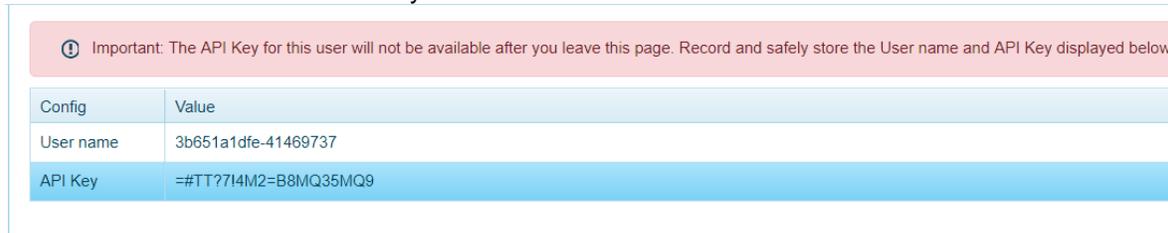
Search: Provide at least 3 char.

	Tracking ID	Common Name	Days Until Expiry
Choose this certificate	304465	5678.testcertificates.com	251
Choose this certificate	311482	12345.example.com	582
Choose this certificate	309986	5678.testcertificates.com	288

4. In the **Add API Key** panel, click **Generate Credentials**.



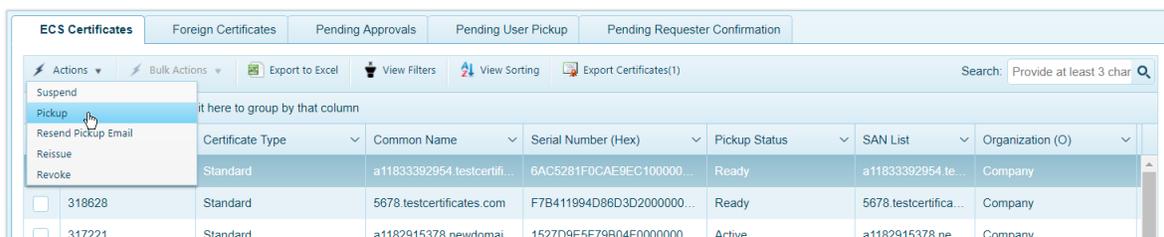
Record the user name and API Key.



Attention: The user name and API key are not available after you leave this page. Be sure to obtain them before proceeding.

5. Download the certificate files.

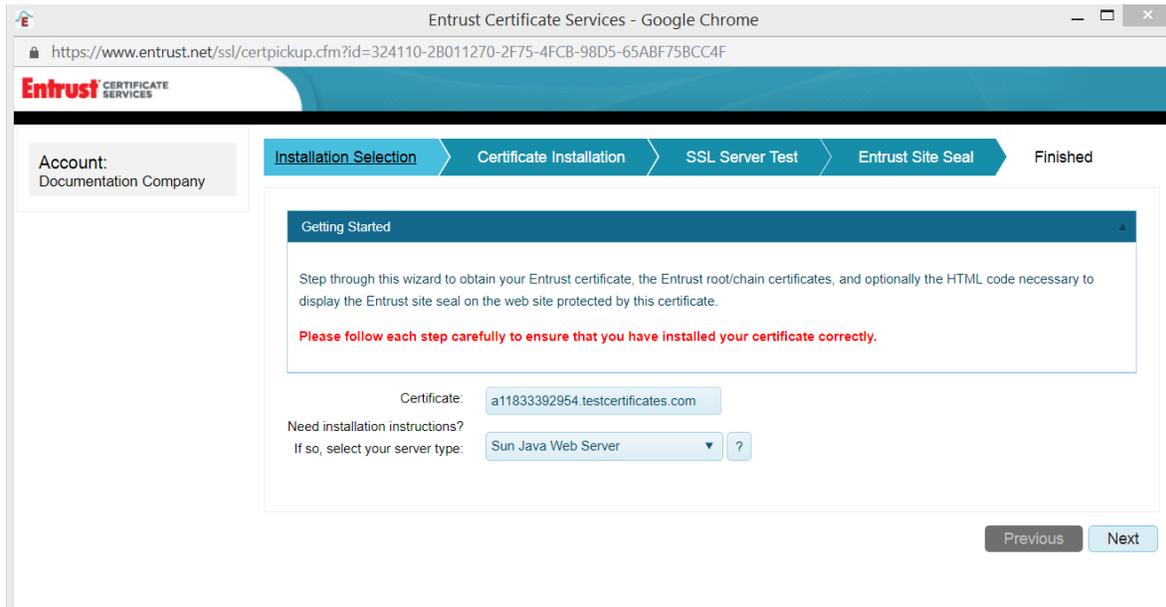
a. From within the ECS portal, click on **Certificates > Managed Certificates**.



b. Select the ECS Certificates tab and locate the SSL certificate created above.

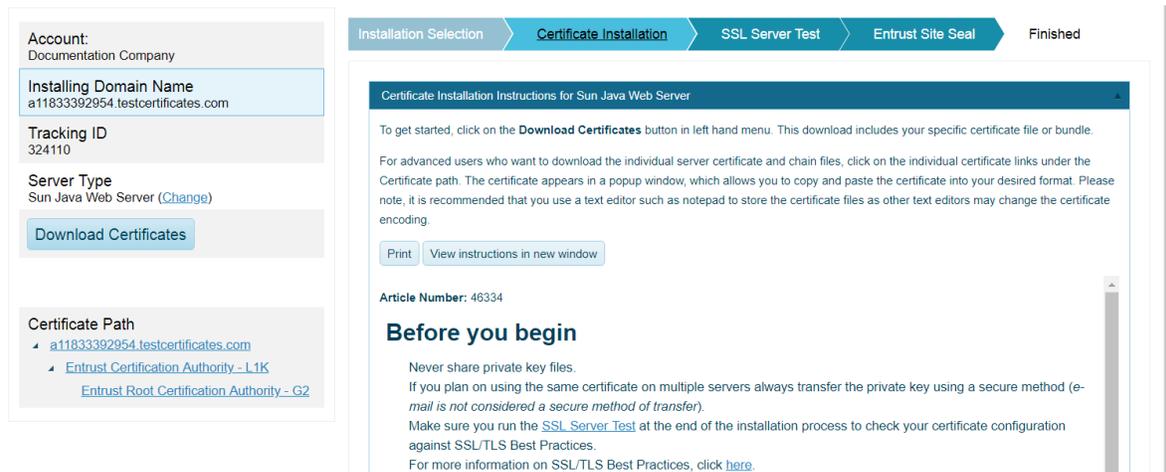
c. Select the certificate and select **Pickup** certificate from the **Actions** drop-down menu.

d. In the certificate pickup pages, choose **Sun Java Web Server** as the Server type and click **Next**.



e. Click **Next**.

f. Click on **Download Certificates** to download the *CertificateBundle.p7b* file.



6. Import the certificate and chain into the Java key store.

```
ubuntu@ubuntu:~$ keytool -import -trustcacerts -alias servicenow -file
CertificateBundle.p7b -keystore servicenow.jks
```

When you install and configure the application you will upload the .jks file (in this example, *servicenow.jks*) and provide the username and password for the API account.