Installing and configuring the Entrust Certificate Services application

Document issue: 1.0

Date of issue: January 2019

Entrust Datacard™

Contents

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.

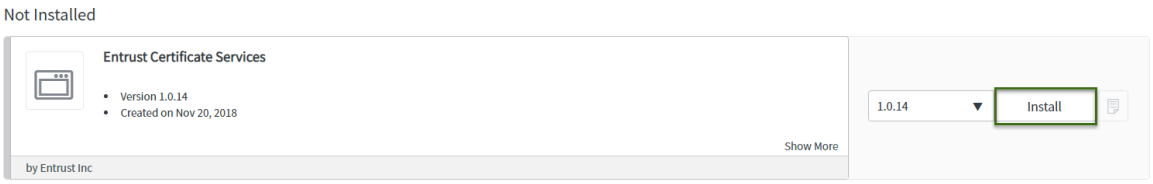
Before you begin

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**.



- 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.

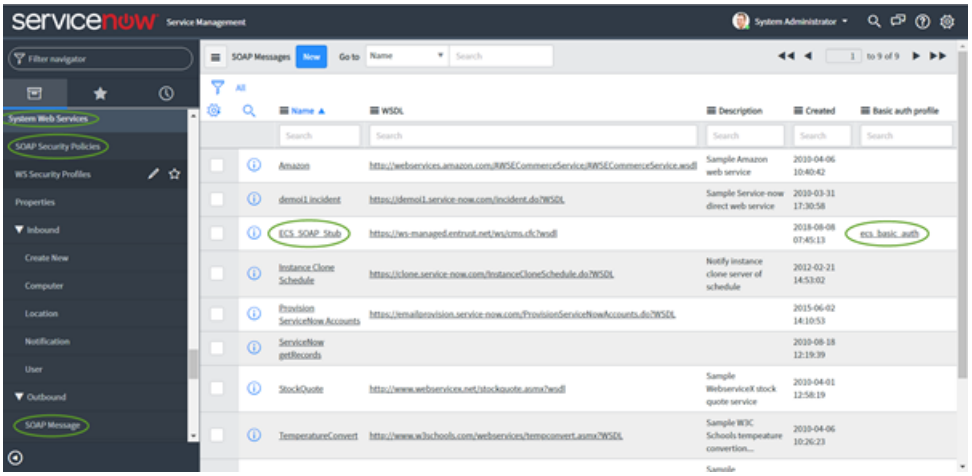
Configuration

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

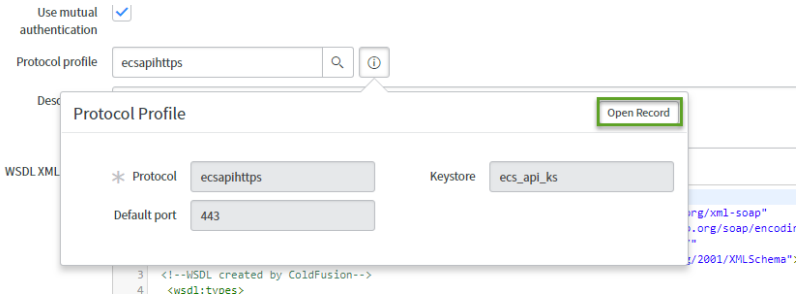
When you have the Entrust Certificate Services API key store, proceed with the following steps:

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

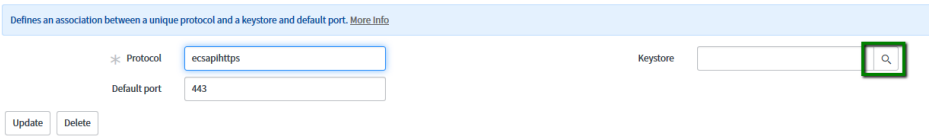


2. In the notification message at the top of the page, click **here** in **To edit this record click here**.
3. Click information (ⓘ) to the right of the **Protocol profile** field.

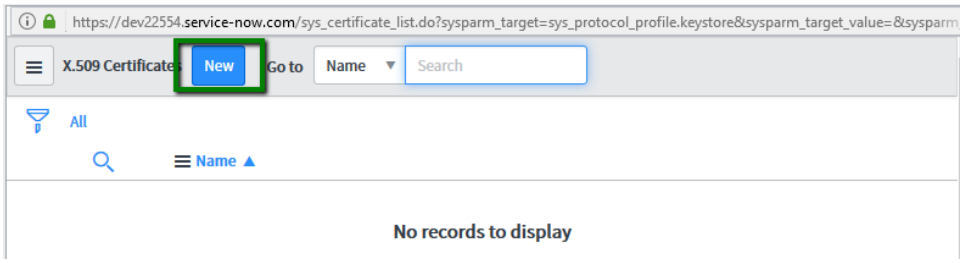
4. On the Protocol Profile configuration page, click **Open Record**.



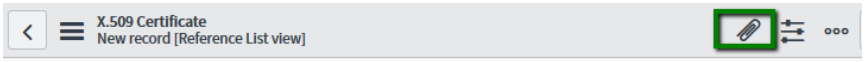
5. In the Protocol Profile page click details (🔍).



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

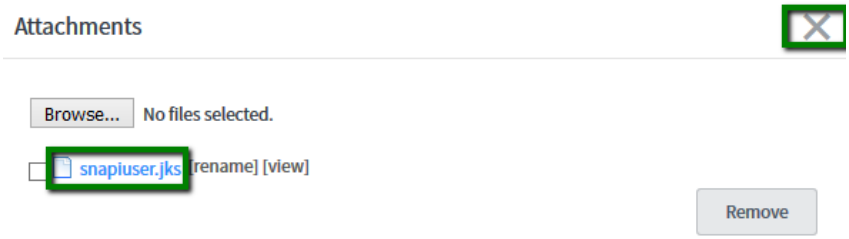


7. On the next page, click attach (📎) to attach a valid API credential from Entrust. The credential must be in either P12/pfx or Java jks format.

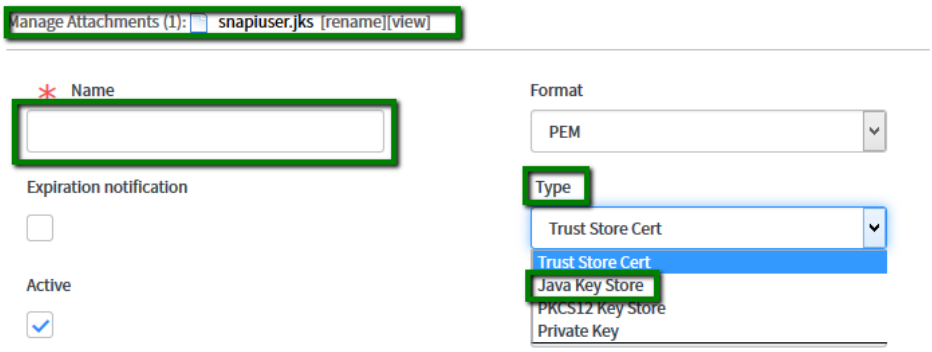


8. In the popup, click **Browse** and navigate to the location of the key store. Select and load the key store file.

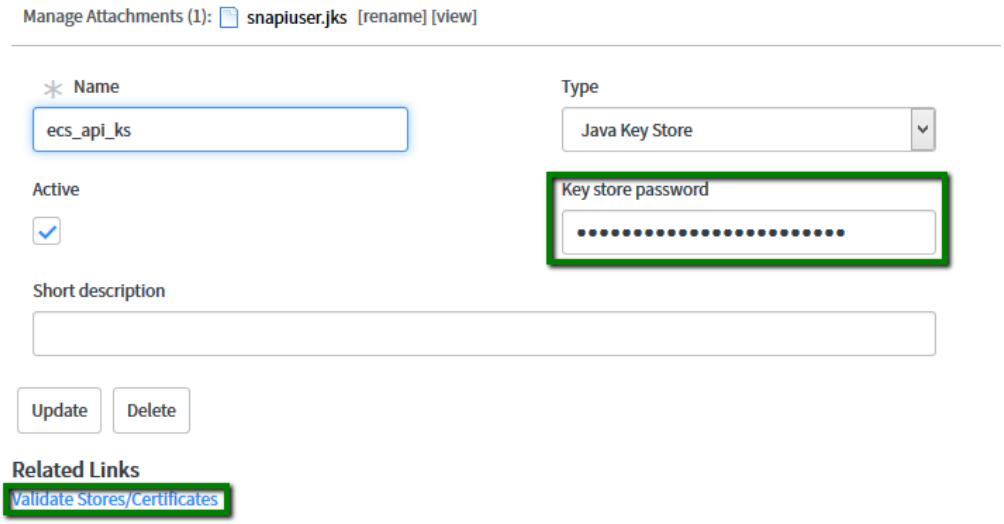
9. When the key store file is attached, close the dialog box.



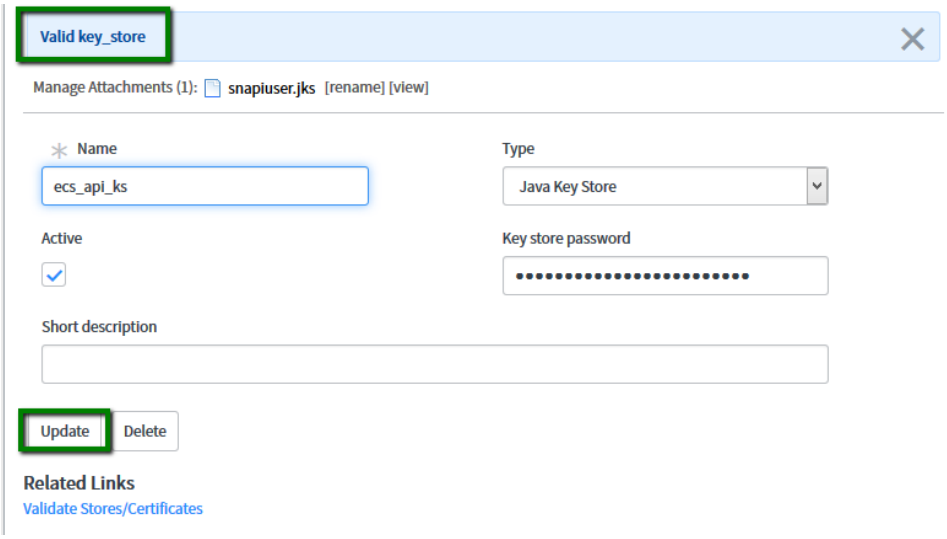
10. Enter the name of the key store and select the key store type. **Java Key Store** is used here as an example.



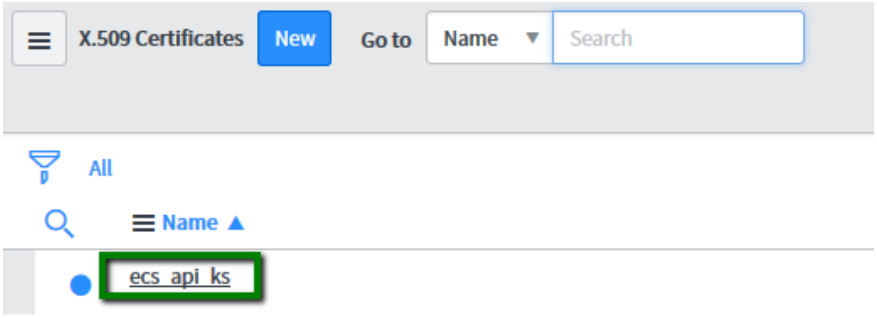
11. Enter the password of the key store and click **Validate Store/Certificates**.



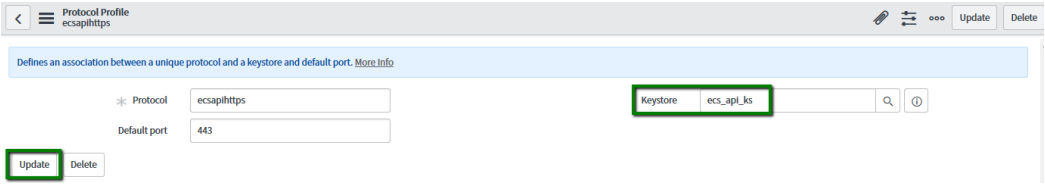
12. When the key store is validated, click **Update** to continue.



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



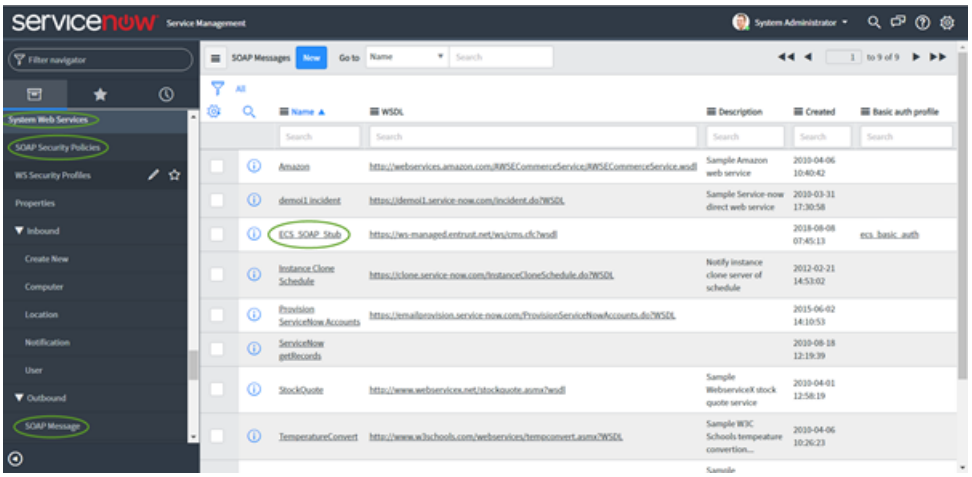
14. The Protocol profile page displays the key store. Click **Update** to save your changes.



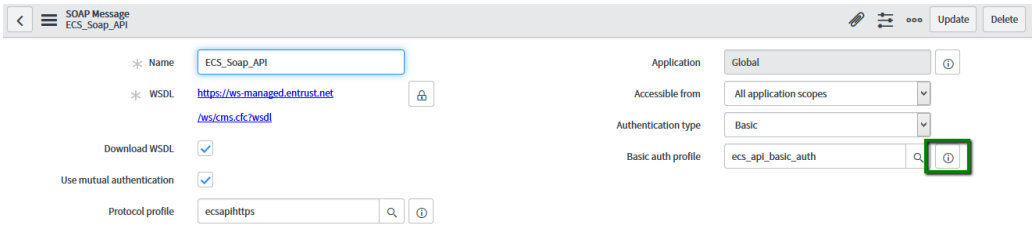
Next, configure the basic authentication profile as outlined in the following procedure.

Configuring the basic authentication profile

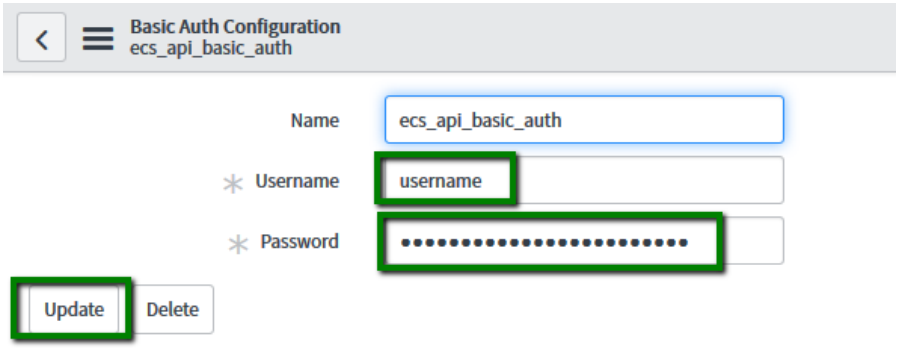
1. Find the Entrust application in the menu. Navigate to **System Web Services** > **SOAP Security Policies** > **Outbound** >**SOAP Message** > **ECS SOAP Stub**



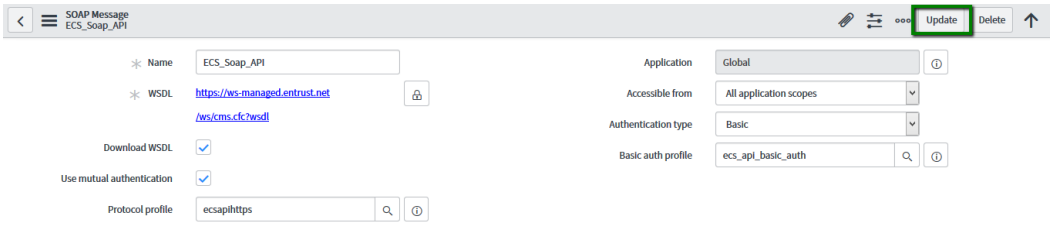
2. On the ECS_SOAP_API page, click information (ⓘ), to the right of the **Basic auth profile** field.



3. 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**.



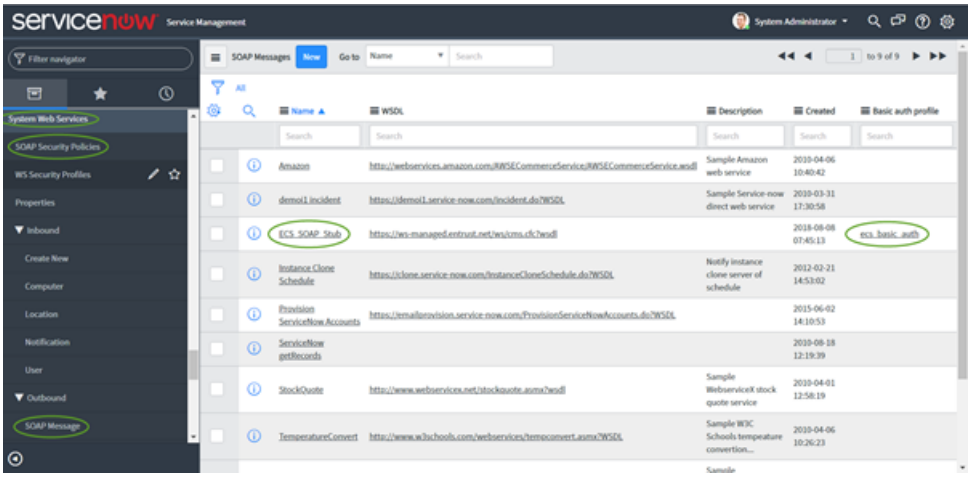
4. Return to the ECS_SOAP_API page (you can use the back button) and click **Update** to commit your changes. Test the connection to the API, as outlined in the next procedure.



Testing the configuration

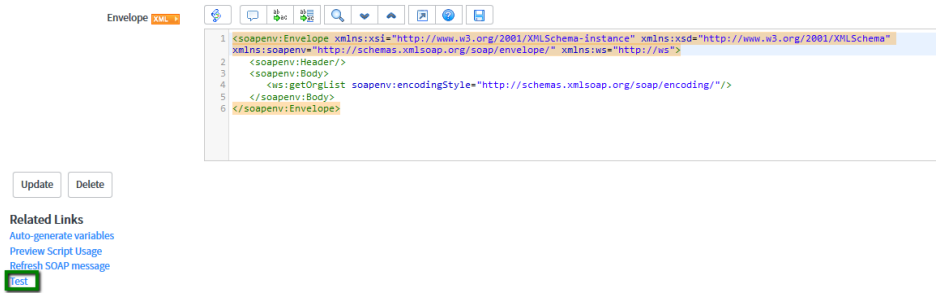
Check that the configuration works as expected.

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

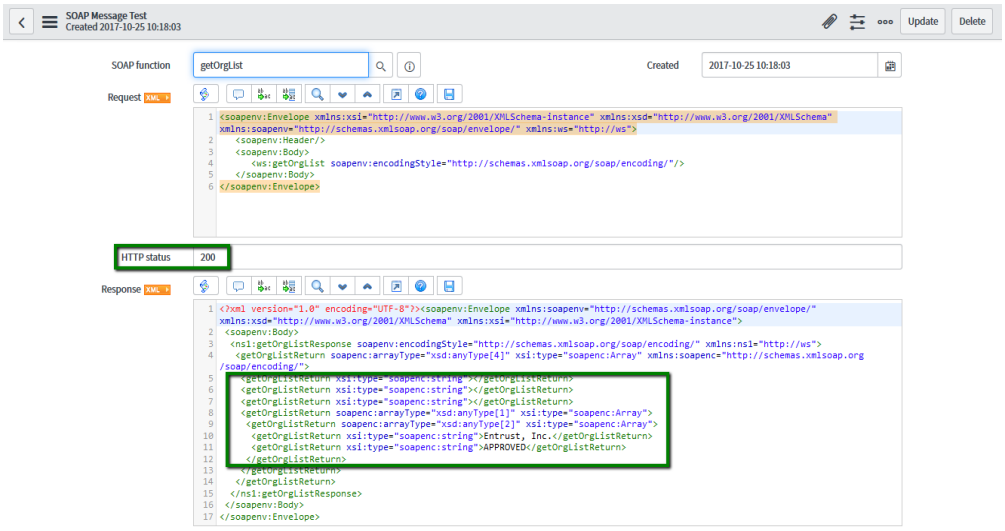


2. On the SOAP Message ECS_Soap_Stub page, scroll down to the bottom and click **getOrgList** in the message list.

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

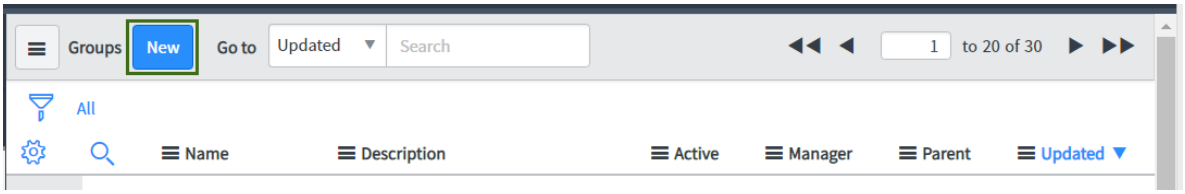
In this section, create groups for specific roles and assign users from your ServiceNow instance to the appropriate group. You can add or remove users from a group at a later date, as needed.

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

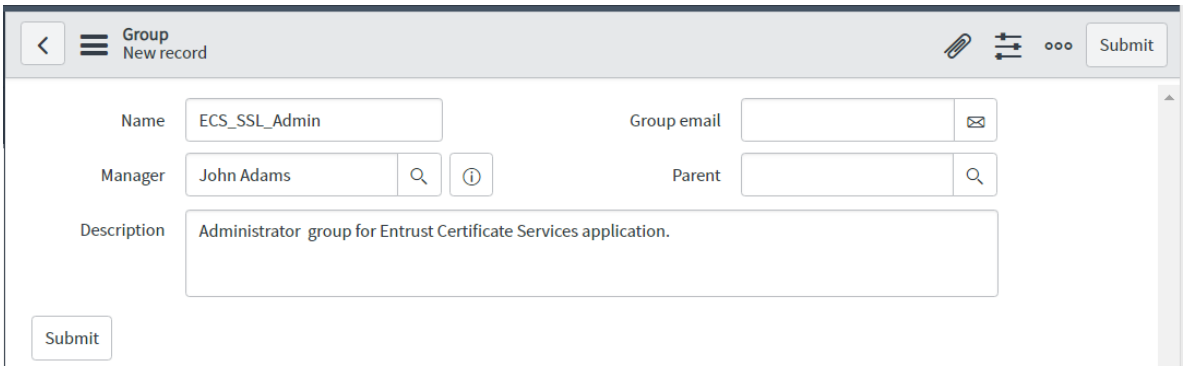
- Administrators have a full set of permissions. They can create, assign, and approve certificate requests as well as download and manage certificates.
- End Users have permission to create certificate requests and approve requests that are assigned to them.

To create user groups

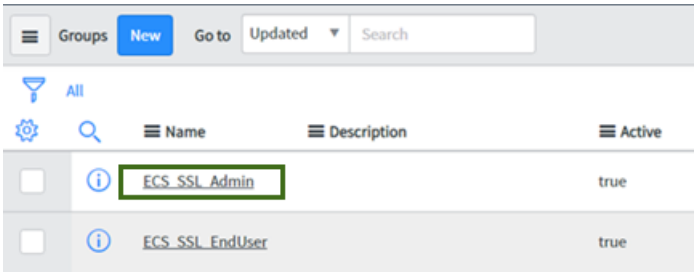
1. Navigate to **System Security** > **Users and Groups** > **Groups**.
2. Click **New** to create a new group.



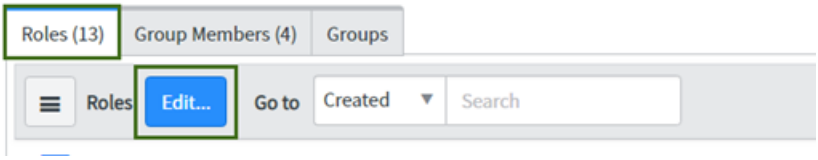
3. Enter a name for the group, group manager, and email address to receive notifications about the group. Add a meaningful description for the group.



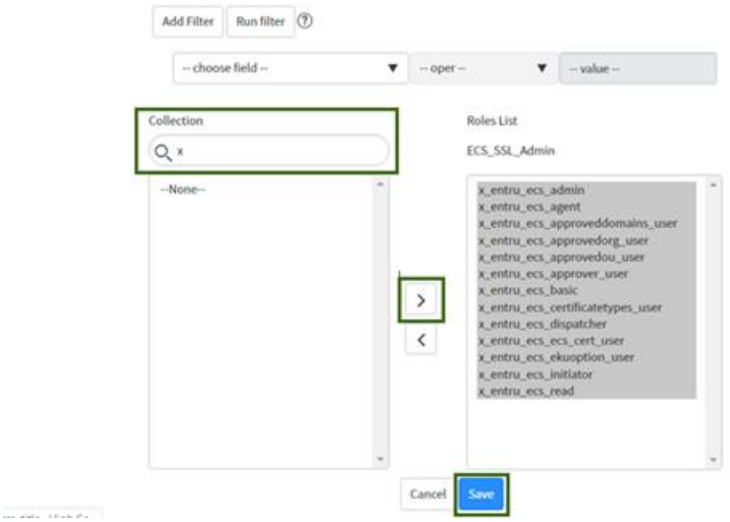
4. Click **Submit**.
5. In the Groups page, add the roles associated with each group.
    a. Click one of the groups that you created: this procedure uses the administrator group.



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



    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**.

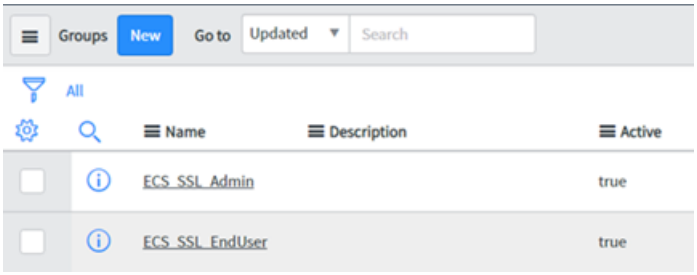
Repeat this procedure for the other group (in this case, the end user group). Give the end user group the following roles only.

- x_entru_ecs_basic
- x_entru_ecs_read
- x_entru_ecs_ecs_cert_user
- x_entru_ecs_ekuoption_user
- x_entru_ecs_approvedorg_user
- x_entru_ecs_approvedou_user
- x_entru_ecs_approveddomains_user

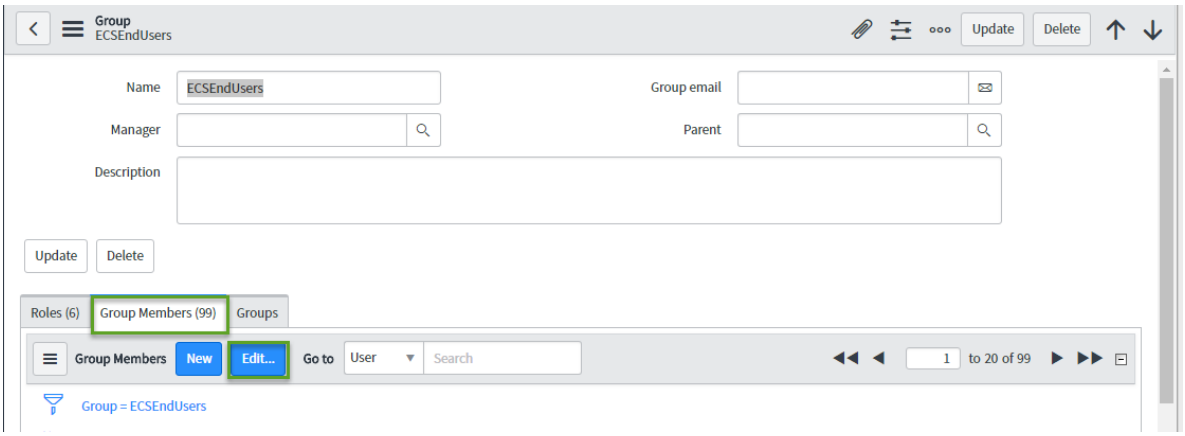
Assign users to your groups as outlined in the following procedure.

To assign users to Certificate Services roles

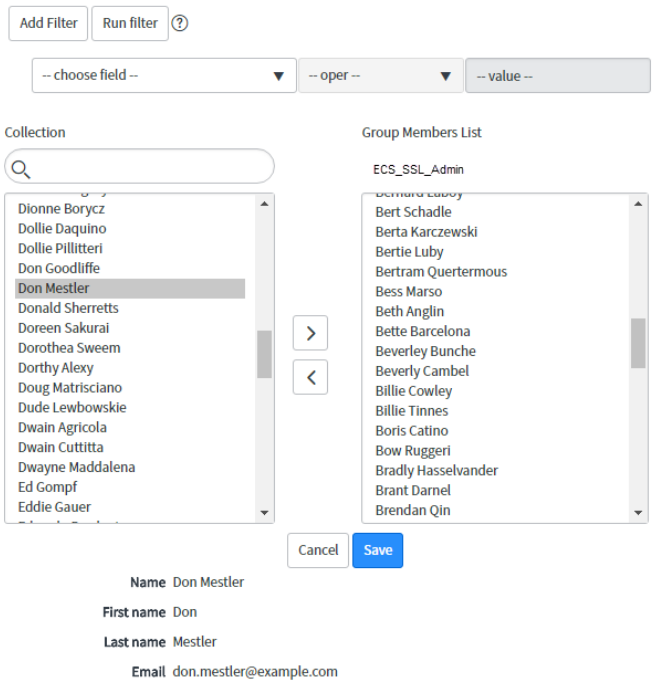
1. Navigate to **System Security** > **Users and Groups** > **Groups**.



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



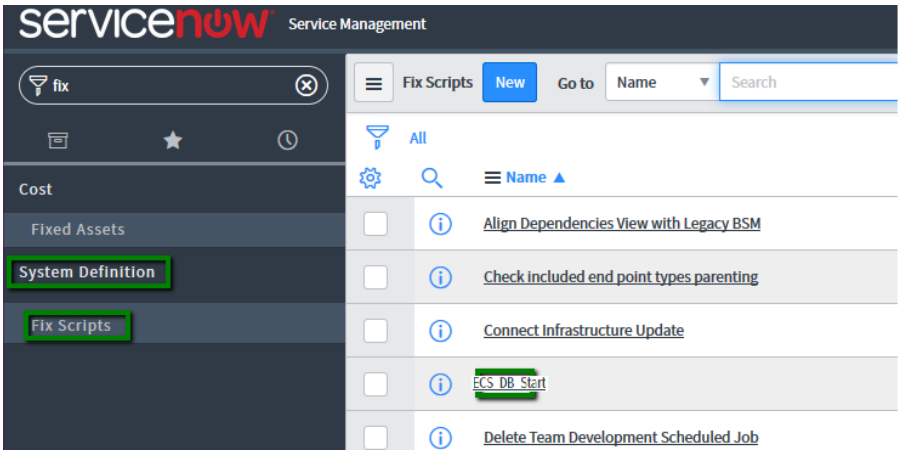
4. Select the users for this group and use the arrow botton to move them to the **Group Members** List.



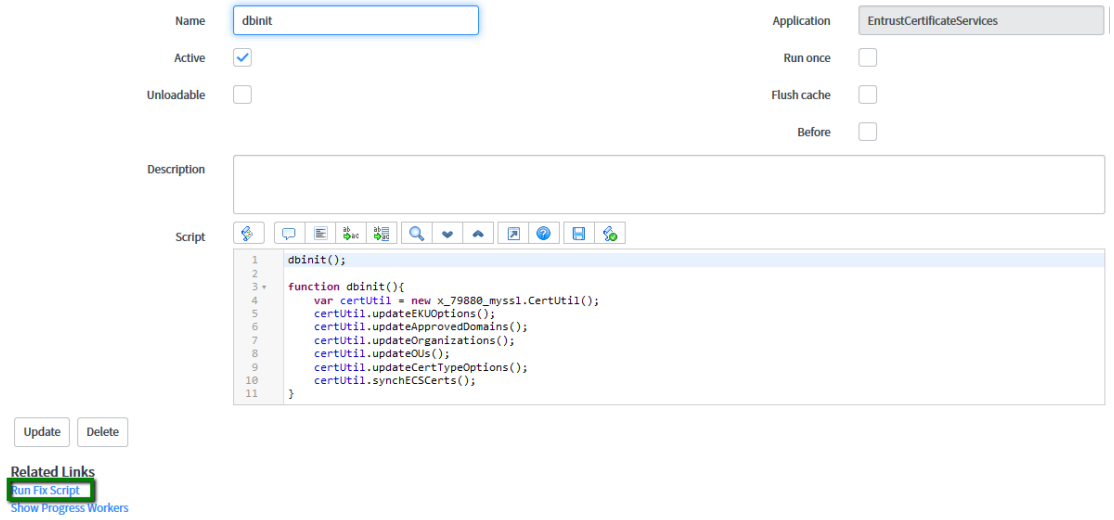
5. Repeat this procedure for the other Certificate Services group.
6. Click **Save**.

Initialize the database

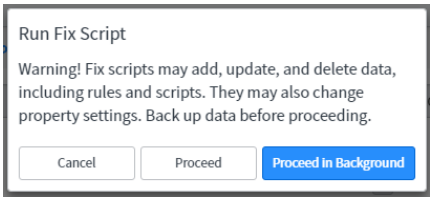
1. Navigate to **System Definition** > **Fix Scripts**. For example, search on **Fix Scripts**. Click **ECS_DB_Start** to initialize the application database records.



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 initilizes 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.

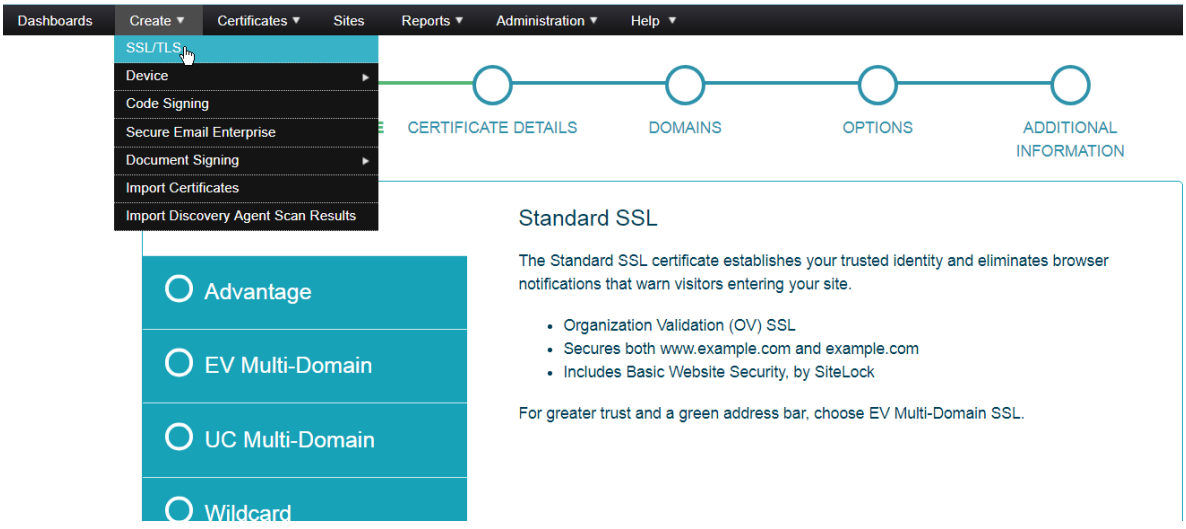
-----BEGIN NEW CERTIFICATE REQUEST----- encoded CSR data in Base64 format ----- END NEW CERTIFICATE REQUEST-----

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).



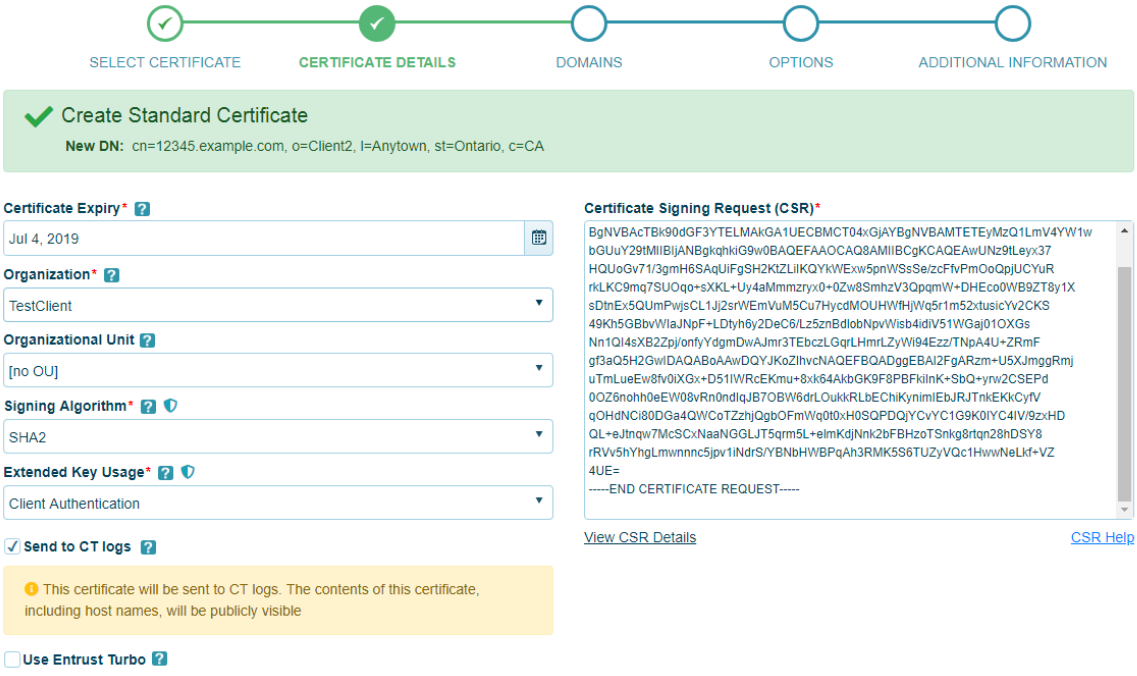
3. Click **Next**.

4. Fill in the following fields:

- Certificate Expiry: Select the desired expiry date.

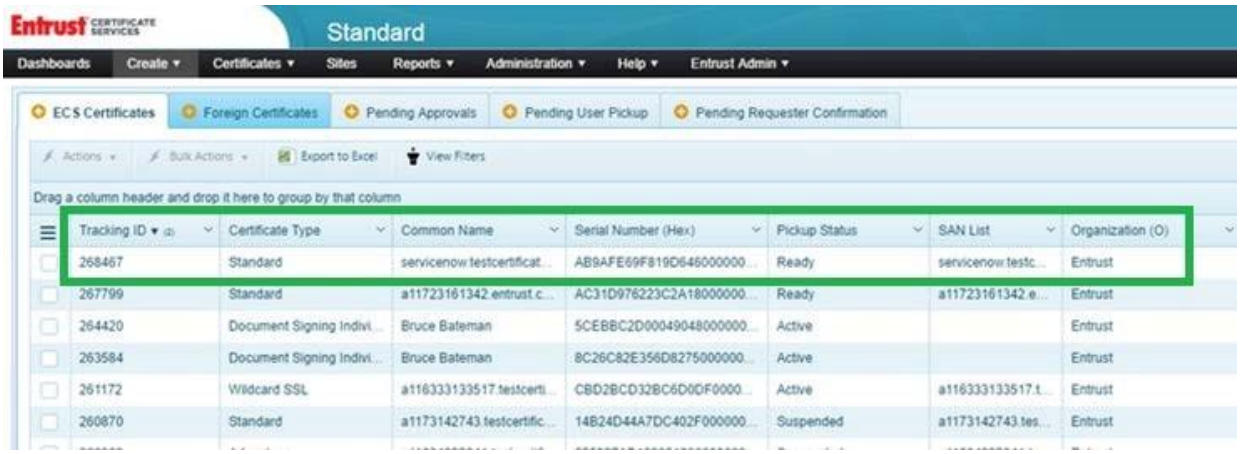
  Note: If the certificate expires, the Certificate Services ServiceNow application will no longer be able to able to access the Certificate Services Enterprise API.

- **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.



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.

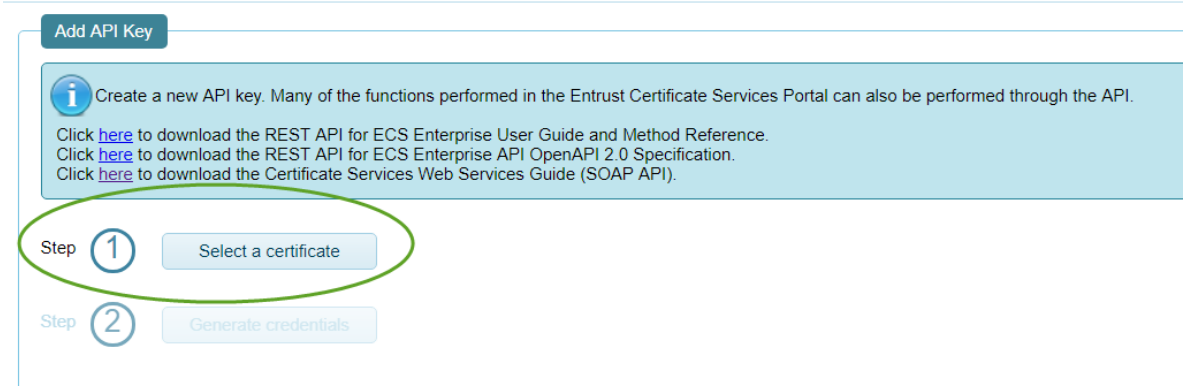
- Your new certificate should appear at the top of the list of ECS Certificates. Record the Tracking ID of this certificate for use in the next section.



Create a new API user

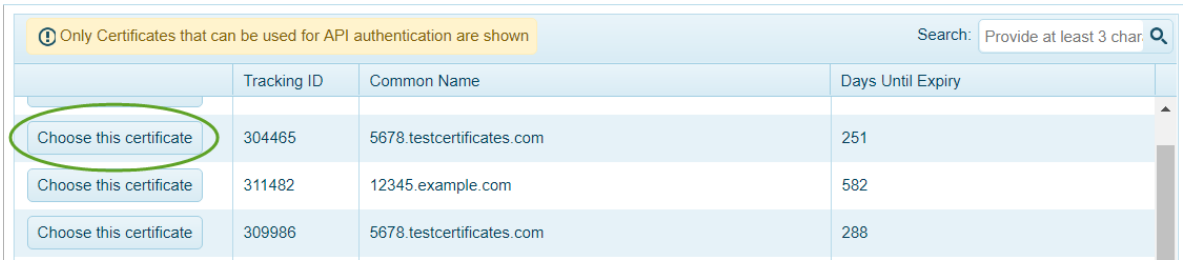
This is the identity that the Certificate Services ServiceNow application uses to authenticate to the Certificate Services web service.

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**.

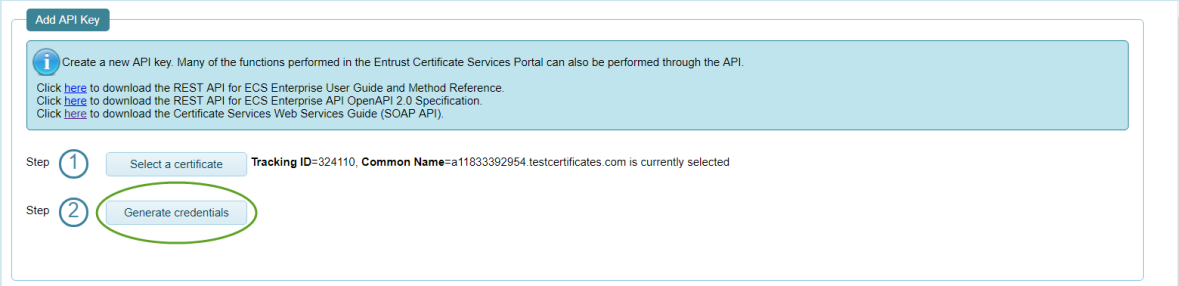


A list of certificates with client authorization opens.

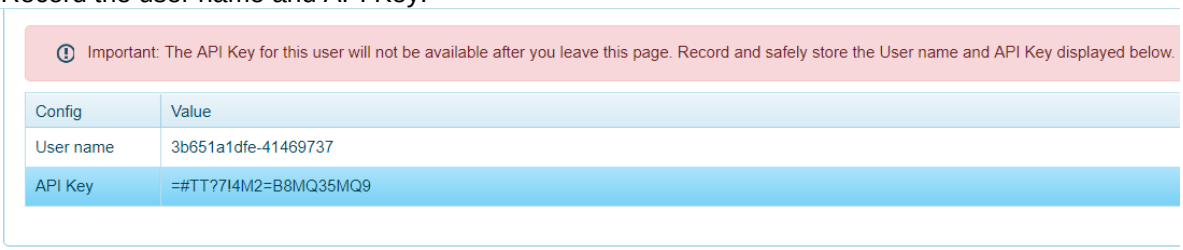
3. Scroll to the certificate that you created for this API account. Click **Choose this certificate**.



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

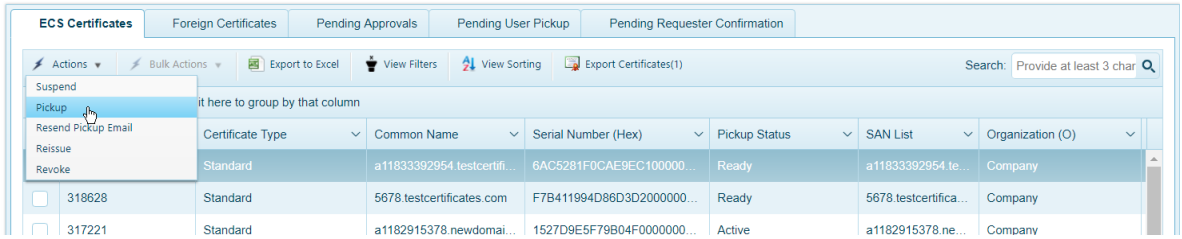


Record the user name and API Key.

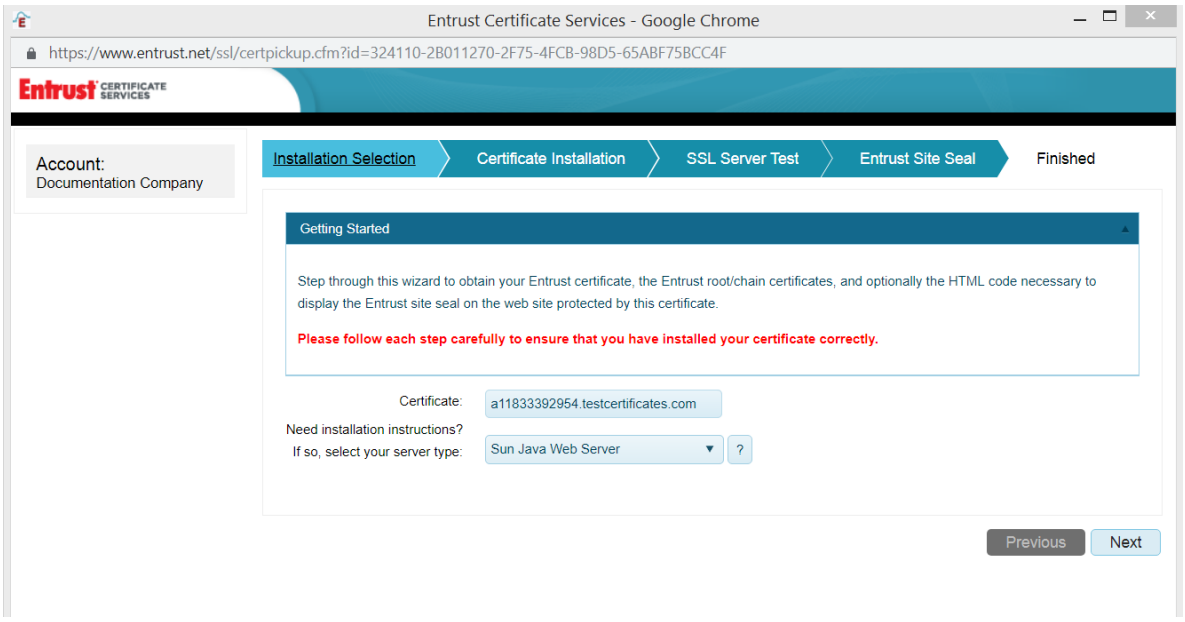


Attention: The user name and API key are not available after you leave this page. Be sure to obtain them before proceeding.

5. Download the certificate files.
    a. From within the ECS portal, click on **Certificates** > **Managed Certificates**.

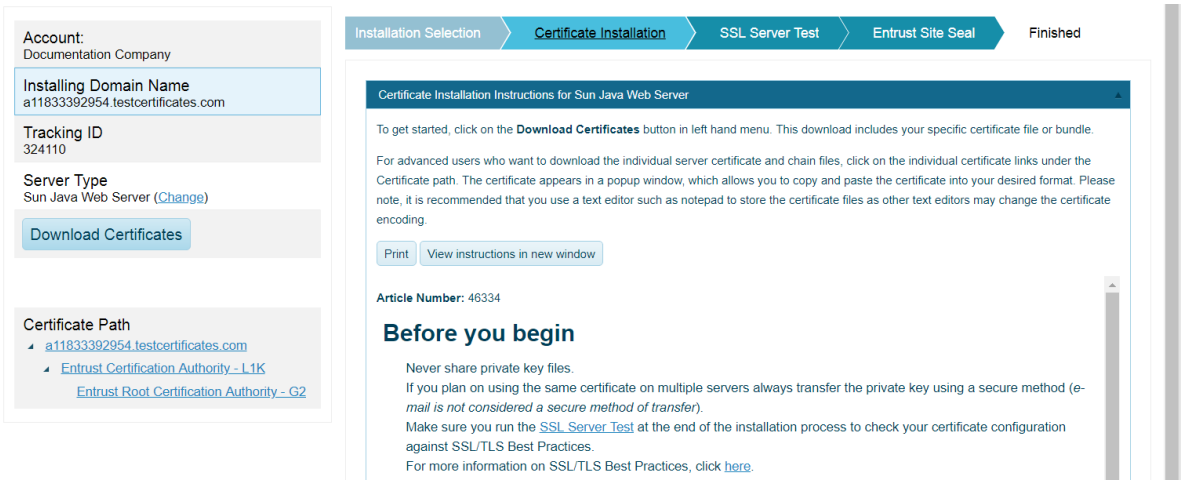


    b. Select the ECS Certificates tab and locate the SSL certificate created above.
    c. Select the certificate and select **Pickup** certificate from the **Actions** drop-down menu.
    d. In the certificate pickup pages, choose **Sun Java Web Server** as the Server type and click **Next**.



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.