Installing and configuring the Entrust Certificate Manager for ServiceNow

Document issue: 2.3

Date of issue: May 2022

Contents

Audience and guide information

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 for use in PDF format.

Conventions

- *ECS* or *Certificate Services* may be used to refer to the **Entrust Certificate Services Enterprise portal**.
- *the API* or *ECS API* or *ECS REST API* may be used to refer to the **Entrust Certificate Services Enterprise Rest API**.
- *CAGW* may be used to refer to the Entrust **CA Gateway**.
- *Entrust Certificate Manager* may be used to refer to the **Entrust Certificate Manager for ServiceNow**.
- *PKI* is used as a general term for the Entrust CA Gateway configuration throughout the guide

ServiceNow version

The Entrust Certificate Manager for ServiceNow is supported on the Orlando, Paris, Rome, and San Diego versions of ServiceNow. This guide is based on the Paris version of ServiceNow.

Introduction

The Entrust Certificate Manager for ServiceNow application is used to btain and manage certificates. Users require an Entrust Certificate Services Enterprise pooling account to create or renew ECS certificates. An Entrust CA Gateway (CAGW) account is required to create or renew PKI certificates.

You can configure the Entrust Certificate Manager for ServiceNow application for either or both options.

- For information about obtaining an Entrust Certificate Services Enterprise (ECS) account see this web page.

Overview of the installation

To configure your ServiceNow account to use the Entrust Certificate Services Enterprise API

1. **(ECS)** From your Certificate Services Enterprise pooling account, create a Certificate Services Web Service (API) account to use with ServiceNow.

   AND/OR
   (PKI) Set up a CA Gateway client as described in the Entrust CA Gateway Operations guide to use with the Entrust Certificate Manager for ServiceNow application.

2. Install the Entrust Certificate Manager for ServiceNow application package from the ServiceNow app store.
3. Configure the Entrust Certificate Manager for ServiceNow application to access the Entrust Certificate Services Enterprise API account and/or the Entrust CA Gateway account. To do this:
   - **(ECS and PKI)** Upload the key store for the ECS API account (P12/pfx or Java jks formats only) or that assigned as a PKI (CA Gateway) client. To use the keystore you must supply the keystore password. This keystore is used to establish a secure connection with the API.
   - **(ECS only)** Supply the basic authentication username and password to allow access to the Entrust Certificate Services Enterprise API account.
4. Create Certificate Services groups with specific user roles.
5. Assign users to the Certificate Services groups.
6. Optionally, if you are using domain separation to control the information available to specific users and administrators, configure it to work with Entrust Manager for ServiceNow.

7. Initialize the database.
8. Obtain the User Guide from the ServiceNow App Store by following this link.

Notes:

- If you want to use domain separation and it is not installed on your ServiceNow instance, apply to ServiceNow to have this feature added. To request domain separation, contact your ServiceNow account manager or make a request through the HI portal. To use domain separation, install it before you install and configure the Entrust Certificate Manager for ServiceNow.

- CMDB (Configuration Management Database) functionality is supported. If you want to use CMDB, see **Prerequisites for CMDB functionality** in the next section.

Before you begin

Creating an API administrator account

ECS

If you have not yet created the API administrator account, do so before beginning the installation. From your Entrust Certificate Services subscription (pooling) account, create a Certificate Services Web Service (REST API) account to use with ServiceNow. If you do not know how to create this type of account, see the guide linked below for instructions. You will need the user ID and password for your ECS Enterprise account to access this guide.
https://cloud.entrust.net/EntrustCloud/documentation/Rest_API_Guide.pdf

PKI

If you are using the Entrust CA Gateway, it should be configured to work with Entrust Certificate Manager for ServiceNow. The Entrust CA Gateway Operations Guide (available from Entrust TrustedCare) contains information about configuring tenants and clients. You will need to use your Entrust TrustedCare credentials to log in to TrustedCare.

Prerequisites for CMDB functionality

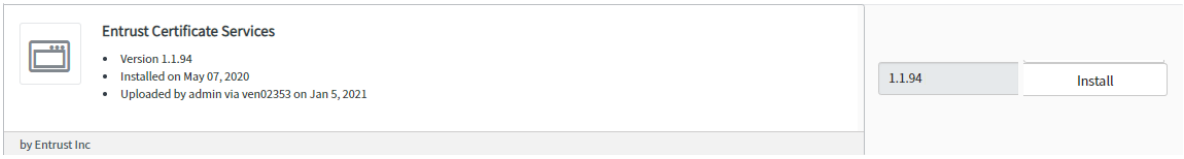
To enable CMDB functionality for the Entrust Certificate Manager for ServiceNow:

1. Activate the plugins listed below on your ServiceNow instance. You can request them from your ServiceNow representative or through the HI portal.
   - Configuration Management (CMDB) - com.snc.cmdb
   - Configuration Management For Scoped Apps (CMDB) - com.snc.cmdb.scoped
2. Install the following application. It is available from the ServiceNow menu **System Application > All**
   - CMDB CI Class Models - sn_cmdb_ci_class

Installing Entrust Certificate Manager for ServiceNow

To install or upgrade the application

1. Navigate to **System Applications**.
2. Find and select Entrust Certificate Services.
3. If this is your initial installation, click **Install**.



Or

If you are upgrading to the next version, select the version from the list and click upgrade. Your configuration information is preserved.

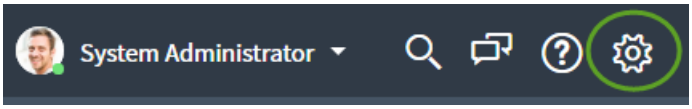
A progress bar appears. A success/failure message appears when the installation or upgrade is completed.

Configuration

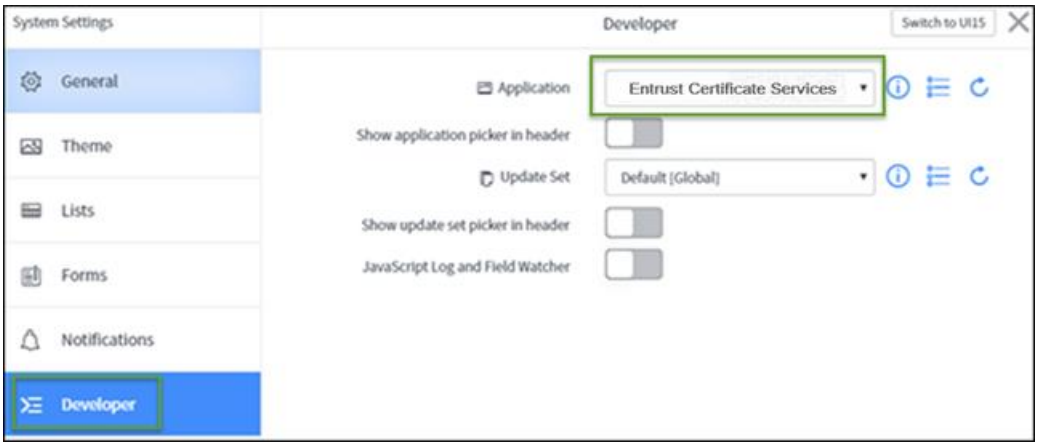
Change the application settings from Global to Entrust Certificate Services

To avoid warning messages and extra steps during configuration change the Application Settings to *Entrust Certificate Services*.

1. Click the settings icon in the upper right corner of the page.



2. In the **Application** pull-down menu, select *Entrust Certificate Services*.



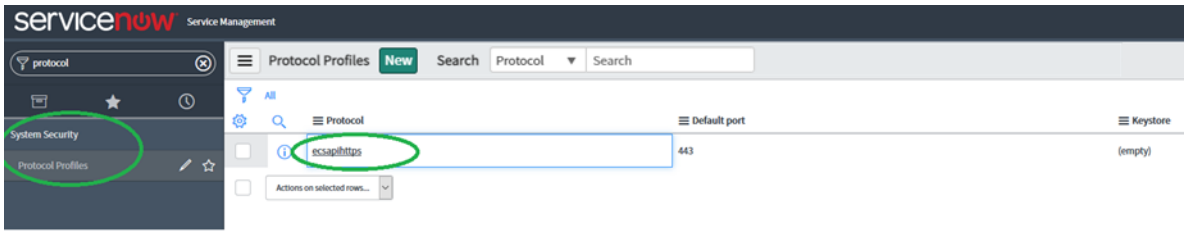
ECS configuration

This section of the guide discusses how to configure the Entrust Certificate Manager for ServiceNow to access and use the Entrust Certificate Services Enterprise REST API (ECS).

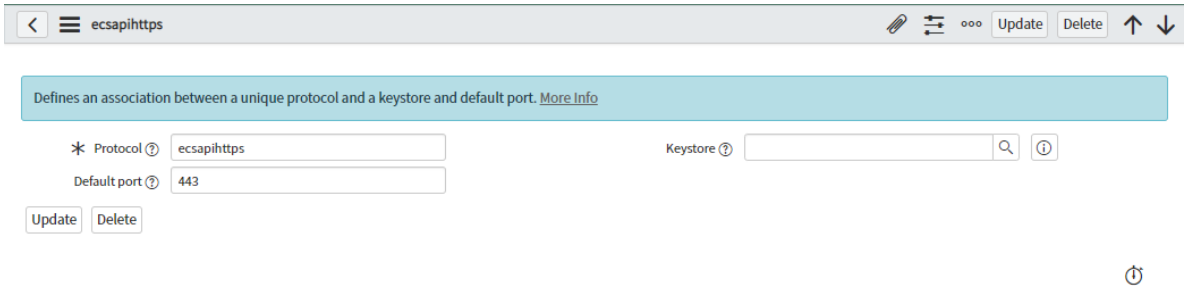
Upload the ECS API administrator account key store

To add the API key store to your protocol profile

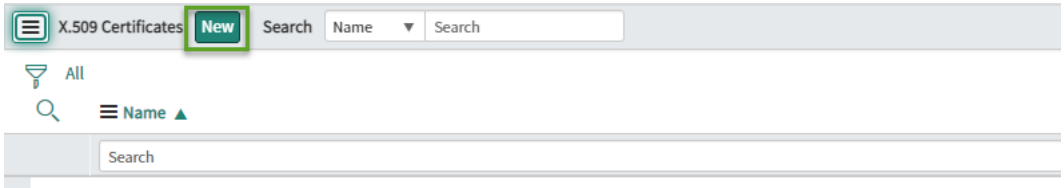
1. Navigate to **System Security** > **Protocol Profiles**.



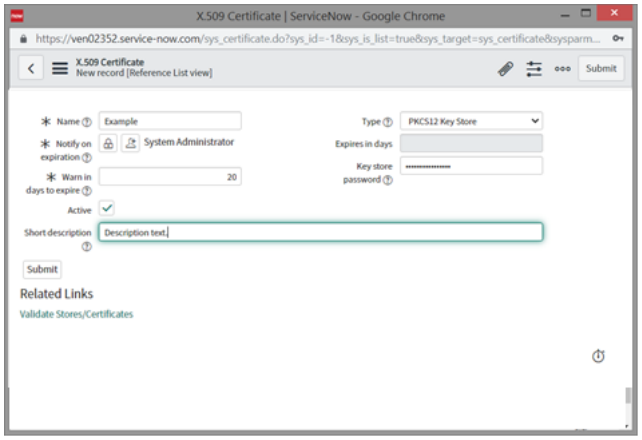
2. Open the *ecsapihttps* record to add your keystore.
3. Click the lookup icon ( ) to the right of the **Keystore** field.



4. In the X.509 Cerificates page, click **New**.



5. In the New Records page:



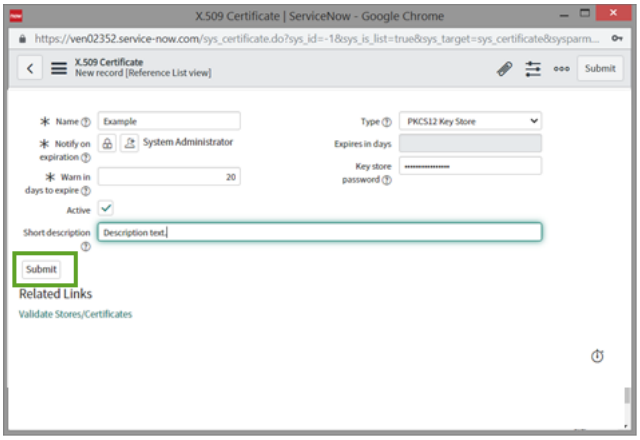
- Enter a name for the record.
- Select the keystore type-- it must be in either P12/pfx or Java jks format.
- Provide the password created for the keystore.

- Enter the expiration information.
- Select **Active**.
- Optionally, enter descriptive text.

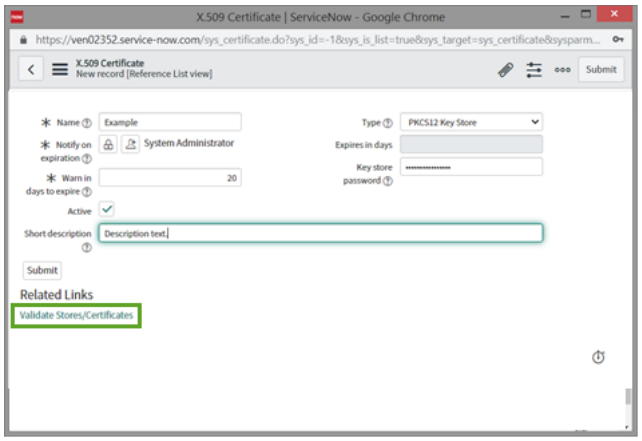
6. To upload the keystore:
   - click attach ( ).

   - In the popup, click **Choose file** and navigate to the location of the keystore. Select and upload the keystore file. It must be in either P12/pfx or Java jks format.

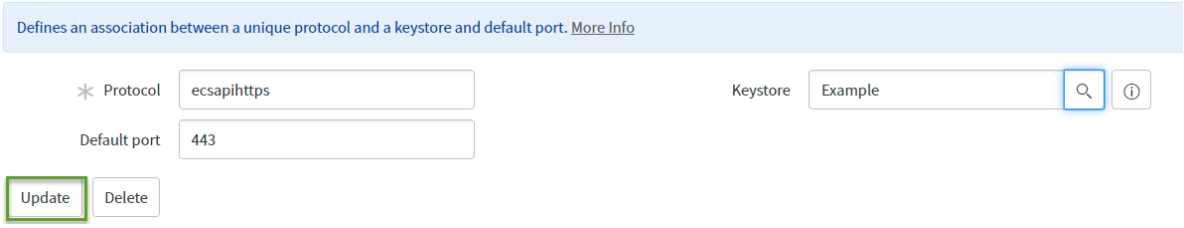
7. In the In the New Records page, click **Submit**.



8. To check the credentials, under **Related Links**, click **Validate stores/Certificates**.



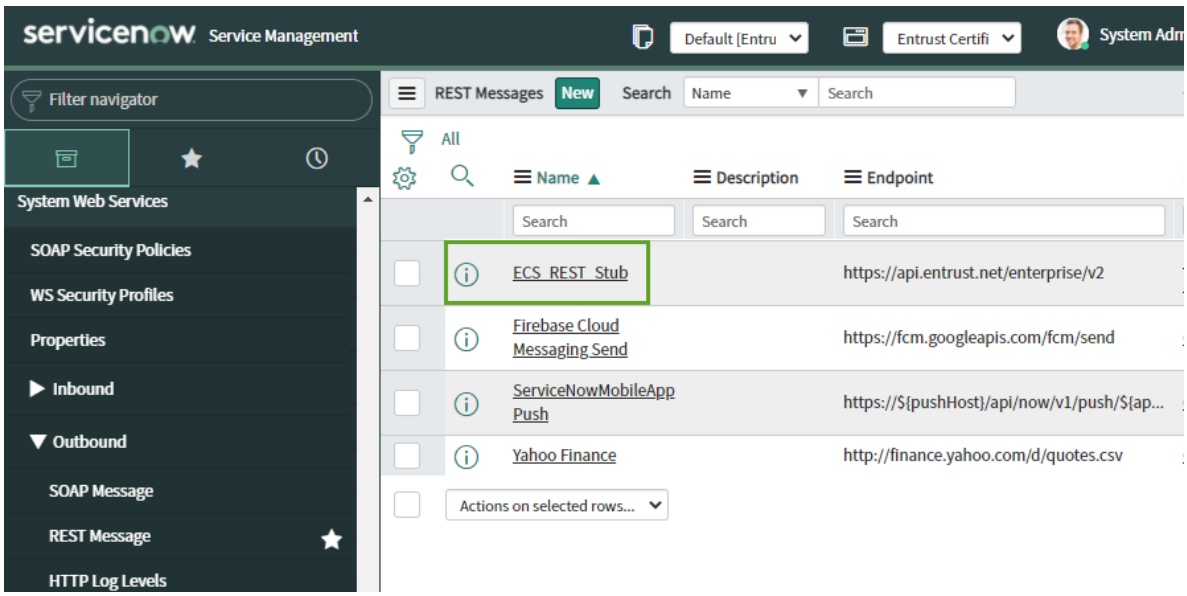
9. In the protocol profile page, click **Update**.



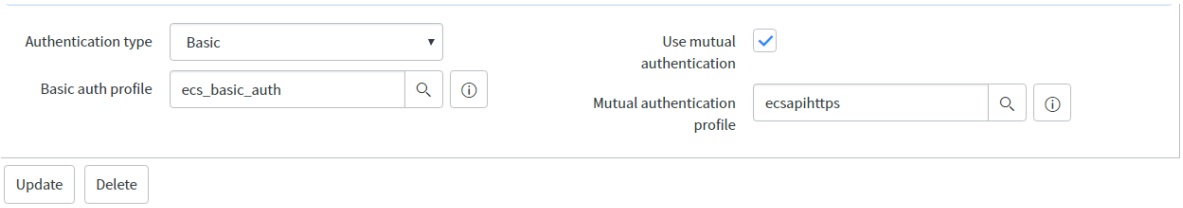
Configure the ECS Protocol Profile

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

1. Find the EntrustDatacard application in the menu. Navigate to **System Web Services** > **Outbound** > **Rest Message**.
2. Select **ECS_REST_Stub** from the list.



3. In the Rest message page select **Use Mutual Authentication**.
4. Click details (🔍) beside the **Mutual authentication profile** field and select the Basic auth profile that you created in the previous procedure.

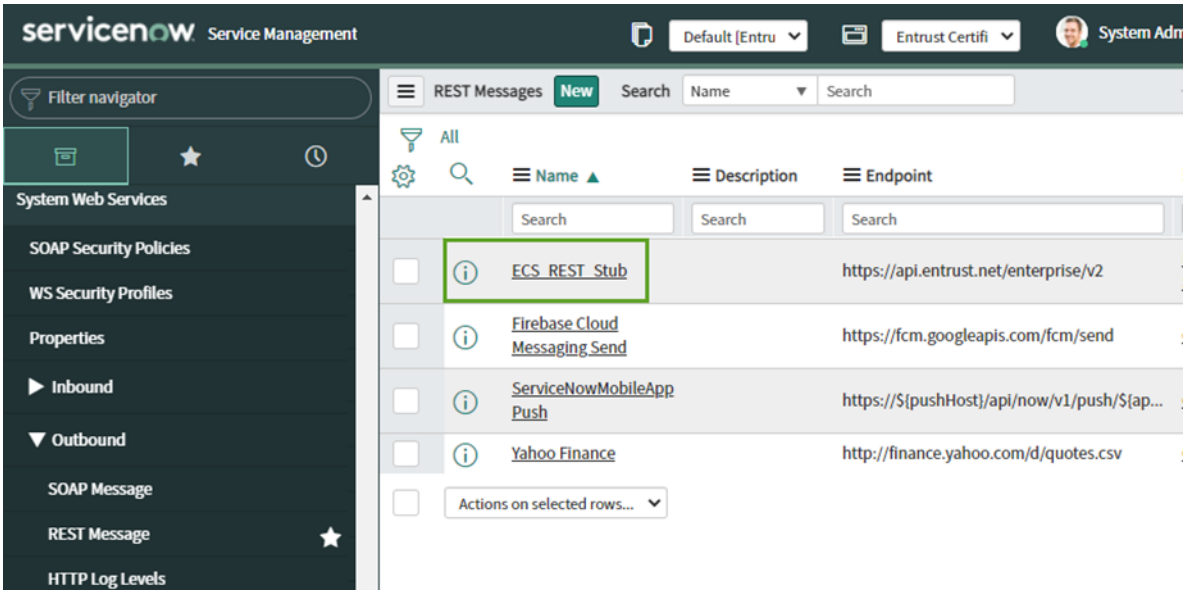


5. Click **Update** to commit your changes.

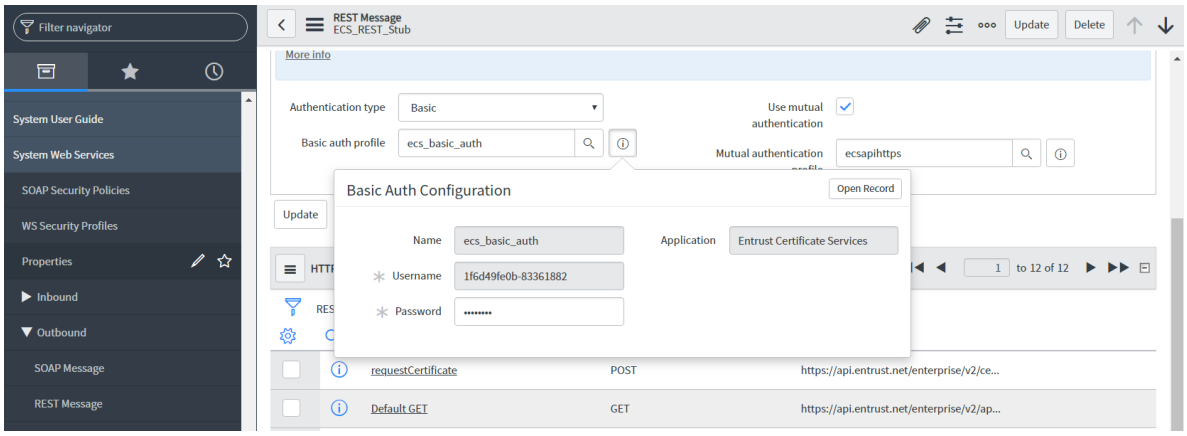
Next, configure the basic authentication profile as outlined in the following procedure.

Configure the ECS basic authentication profile

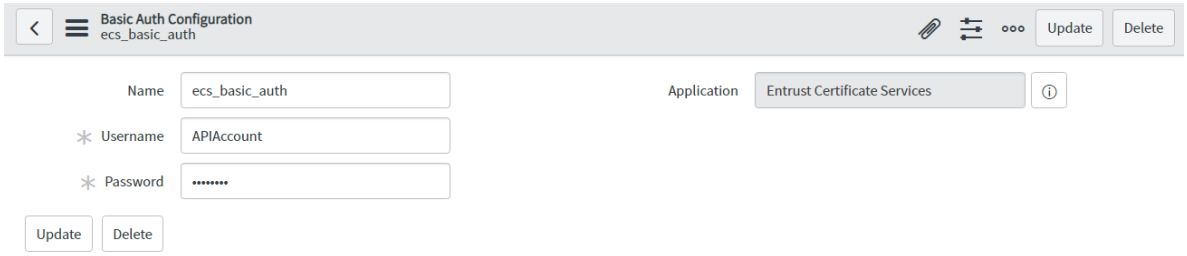
1. Find the Entrust application in the menu. Navigate to **System Web Services** > **Outbound** > **Rest Message**.
2. Click ECS_REST_Stub.



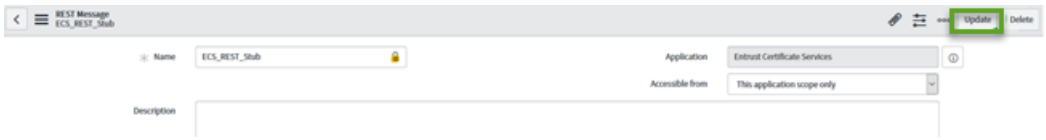
3. On the REST Message page, click information (ⓘ), to the right of the **Basic auth profile** field.



4. Click Open Record.
5. On the Basic Auth Configuration page, enter the username and password for the Certificate Services account. Click **Update**.



6. Return to the ECS_REST_API page and click **Update** to commit your changes.

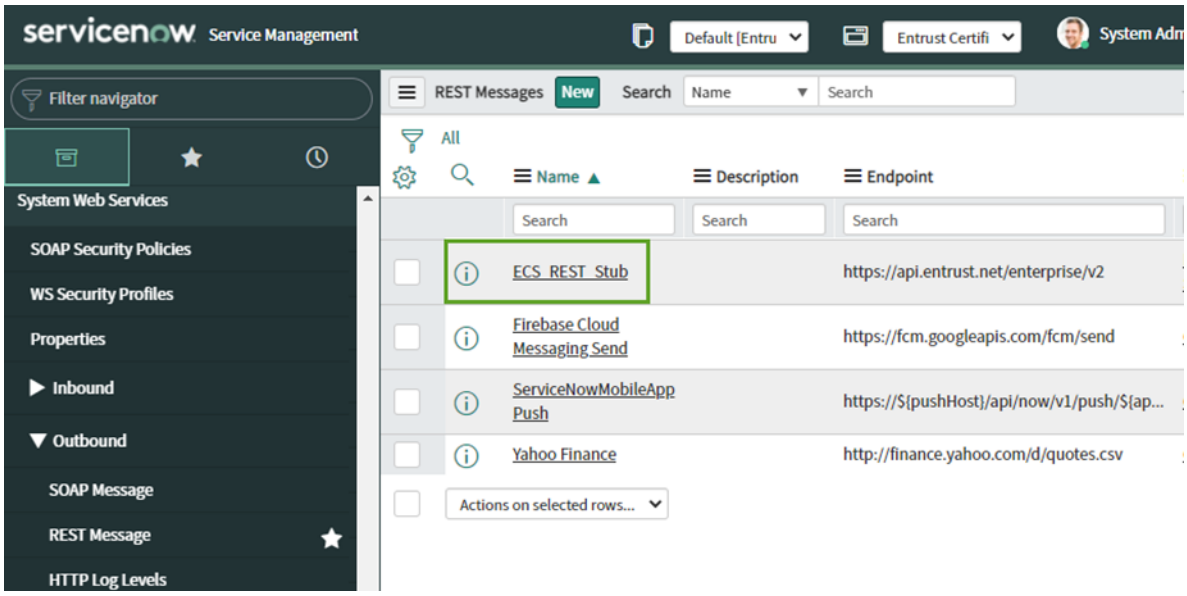


Test the connection to the API, as outlined in the next procedure.

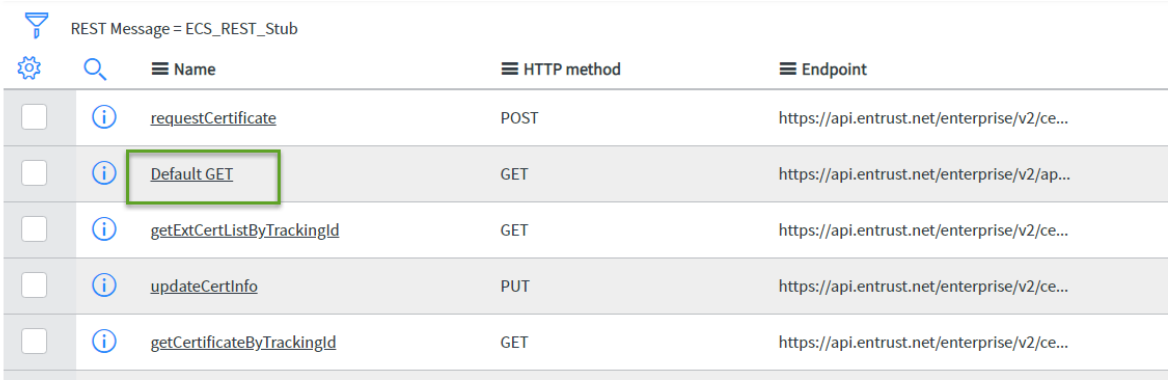
Test the ECS configuration

Optionally, check that the configuration works as expected.

1. On the Rest Messages page, click **ECS_REST_Stub**.



2. On the REST Message ECS_REST_Stub page, scroll down and click **DefaultGET** in the list.



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

> **Note**: If you get errors at this point, return to the previous two procedures and be sure that you correctly configured the Authentication Type and the Basic and Mutual Authentication profile, and that you selected **Use Mutual Authentication**.

PKI (CA Gateway) Configuration (Optional)

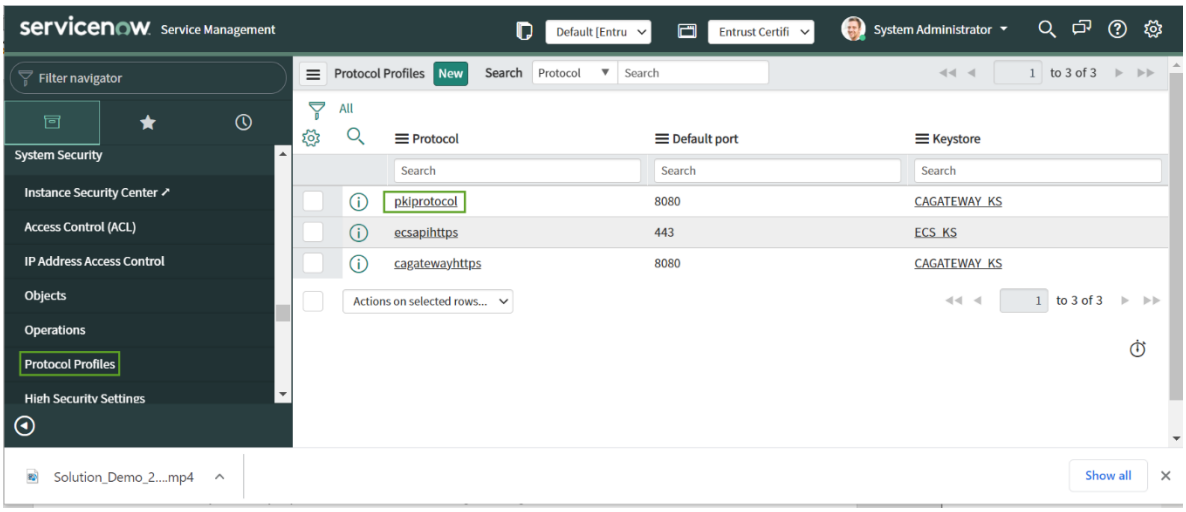
This section of the guide discusses how to configure the Entrust Certificate Manager for ServiceNow to access and use the Entrust CA Gateway API (PKI). If

you are not using the CA Gateway, proceed to the section Create Certificate Manager user groups and assign users.

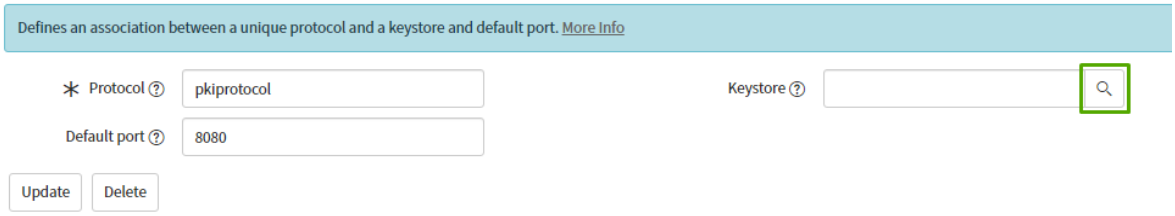
Upload the PKI (CA Gateway) API key store

To add the PKI API key store to your protocol profile

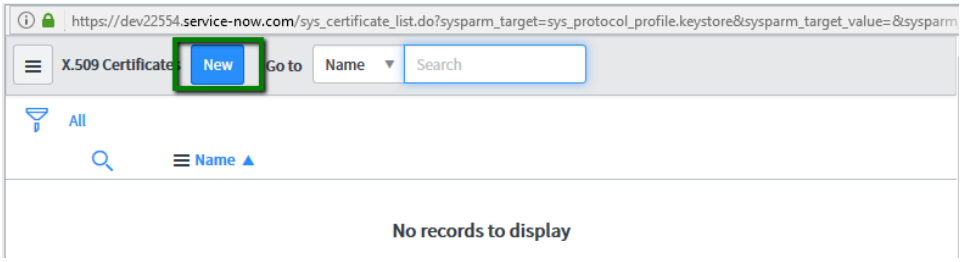
1. Navigate to System Security > Protocol Profiles.



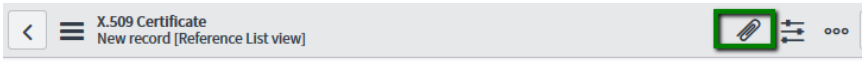
2. Click pkiprotocol.
3. Click the lookup icon (🔍) to the right of the **Keystore** field.



4. In the X.509 Cerificates page, click **New**.

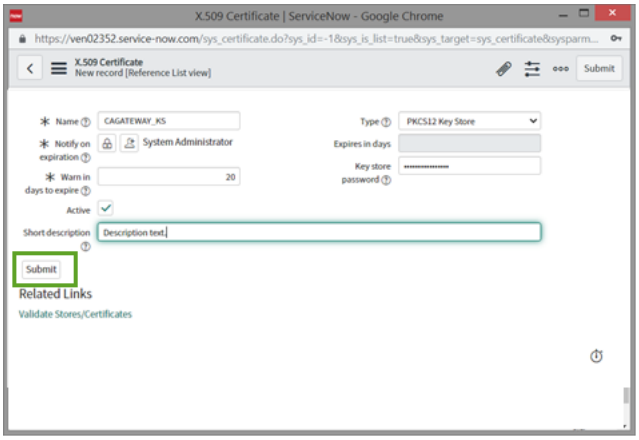


5. In the next page click attach (📎) to attach the PKI API keystore.

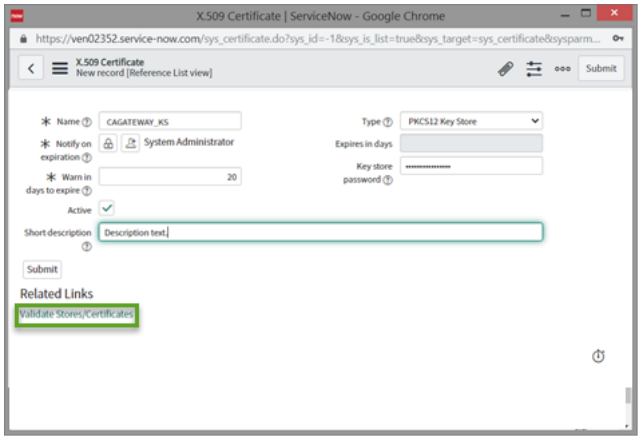


6. In the popup, click **Choose file** and navigate to the location of the keystore. Select and upload the keystore file. It must be in either P12/pfxor Java jks format.

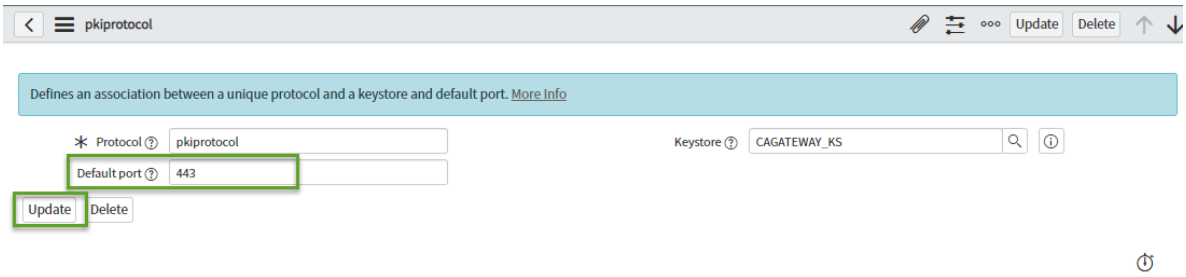
7. Select the keystore type, provide the password for the keystore, and click **Submit**.



8. To check the credentials, under **Related Links**, click **Validate stores/Certificates**.



9. In the protocol profile page, change the **Default port** to the port used by your CA Gateway. Typically this is port 443.

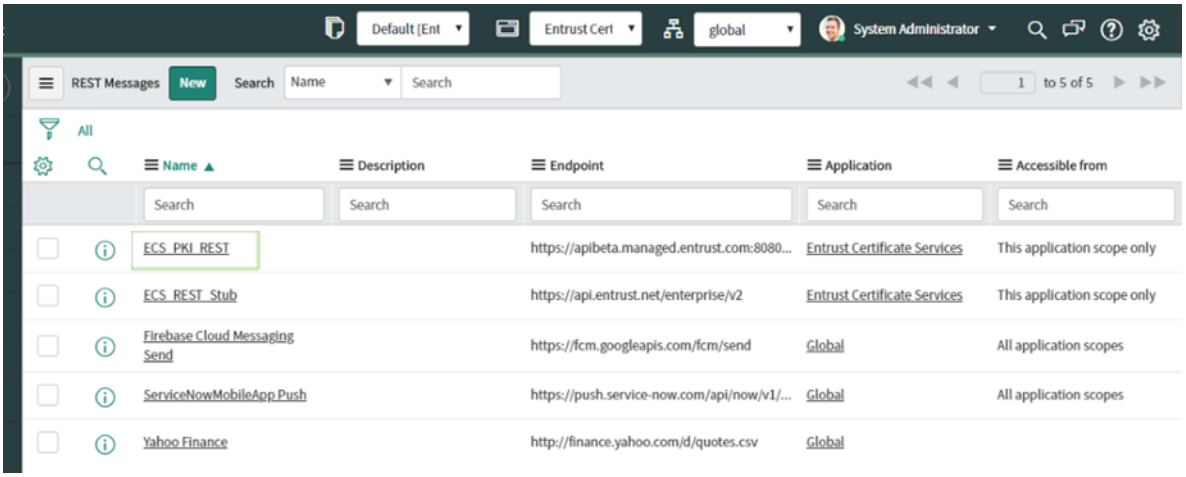


10. Click **Update** to save your changes.

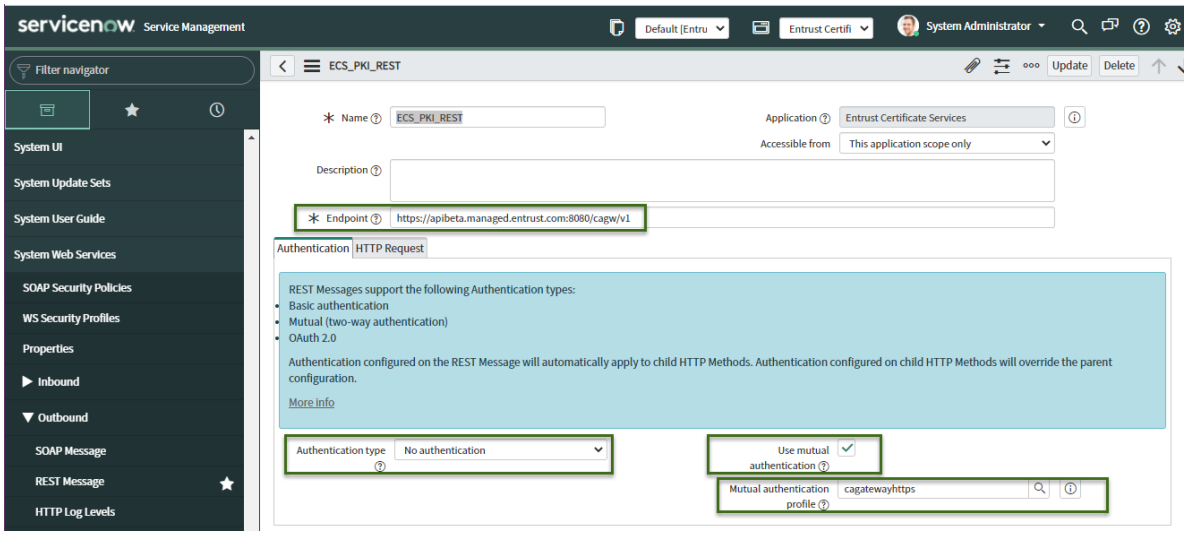
Configure the PKI (CA Gateway) API Protocol Profile

When you have uploaded the PKI API key store for Entrust CA Gateway, proceed with the following steps:

1. Navigate to System Web Services > Outbound > Rest Message.
2. Select ECS_PKI_REST from the list.



3. In the ECS_PKI_REST message page:



a. For Authentication type, select **No authentication**.

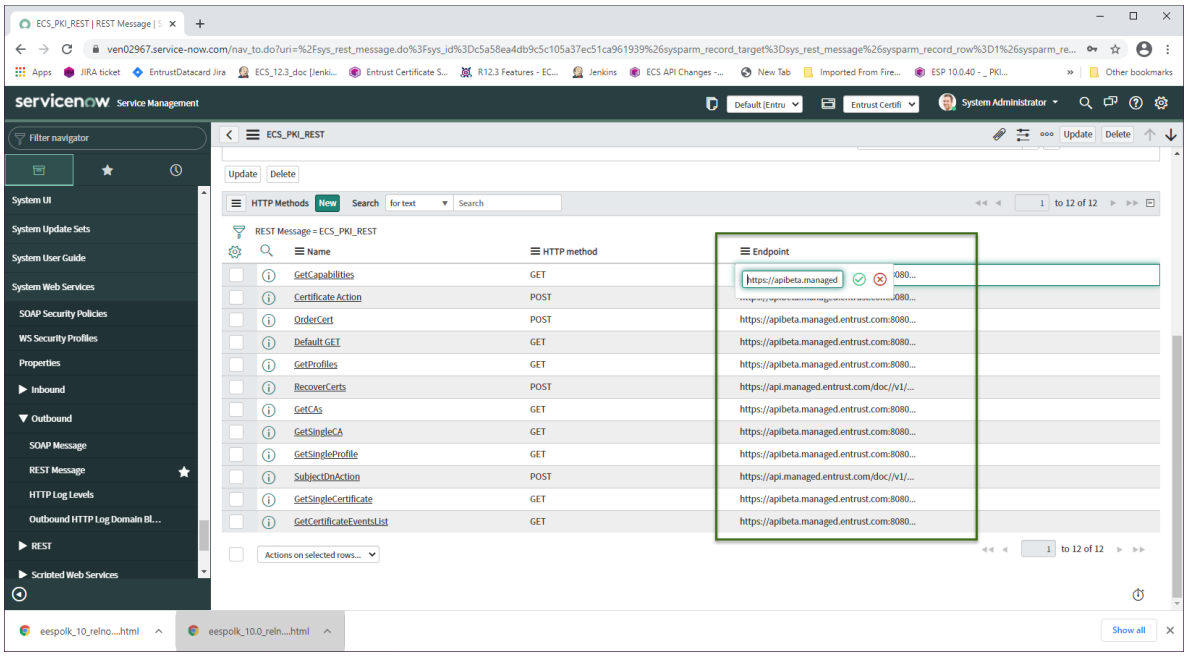
b. Select the Use Mutual Authentication checkbox.

c. Edit the **Endpoint** to use the URL of your CA Gateway.

d. Click details (🔍) beside the **Mutual authentication profile** field and select the protocol profile that you created in the previous procedure.

e. Click the information icon (ⓘ) beside the **Mutual authentication profile** field. Check the protocol information. Be sure that the keystore and port information are correct. If not click Open record and edit the fields.

4. Scroll down the list at the bottom of the page and edit **all** of the Endpoints in the list to use the URL of your CA Gateway. You can double click the endpoint URLs to edit them. Only edit the first part of each endpoint URL (point them to the correct address rather than the default). This step is to ensure that they point to endpoints on the correct CA Gateway.



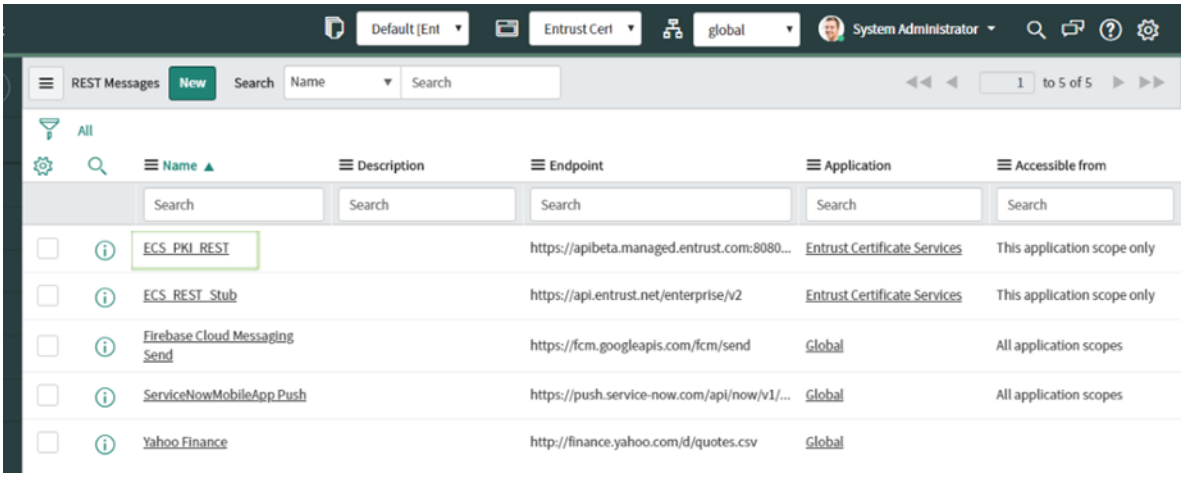
5. Click **Update** to commit your changes.

Next, test the configuration as outlined in the following procedure.

Test the PKI configuration

Optionally, check that the configuration works as expected.

1. On the Rest Messages page, click **ECS_PKI_REST**.



2. On the REST Message ECS_PKI_REST page, scroll down and click **DefaultGET** in the list.

3. Click **Test**.

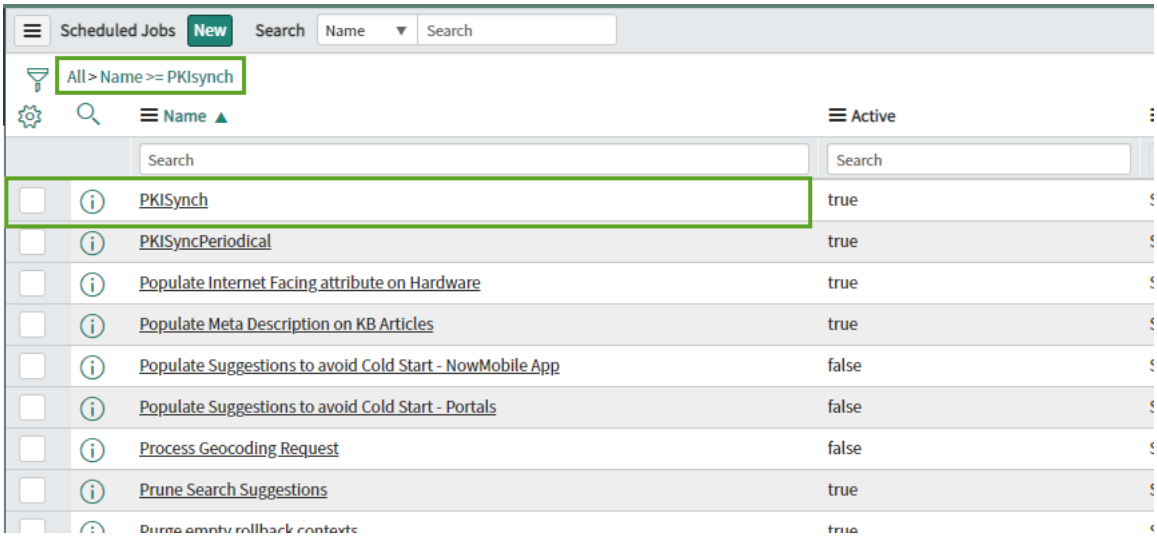
Check the information on the next page. HTTP Status should be 200 and the response should not include any errors.

> **Note**: If you get errors at this point, return to the previous procedures and be sure that you correctly configured the Authentication Type and the Mutual Authentication profile, and that you selected **Use Mutual Authentication**.

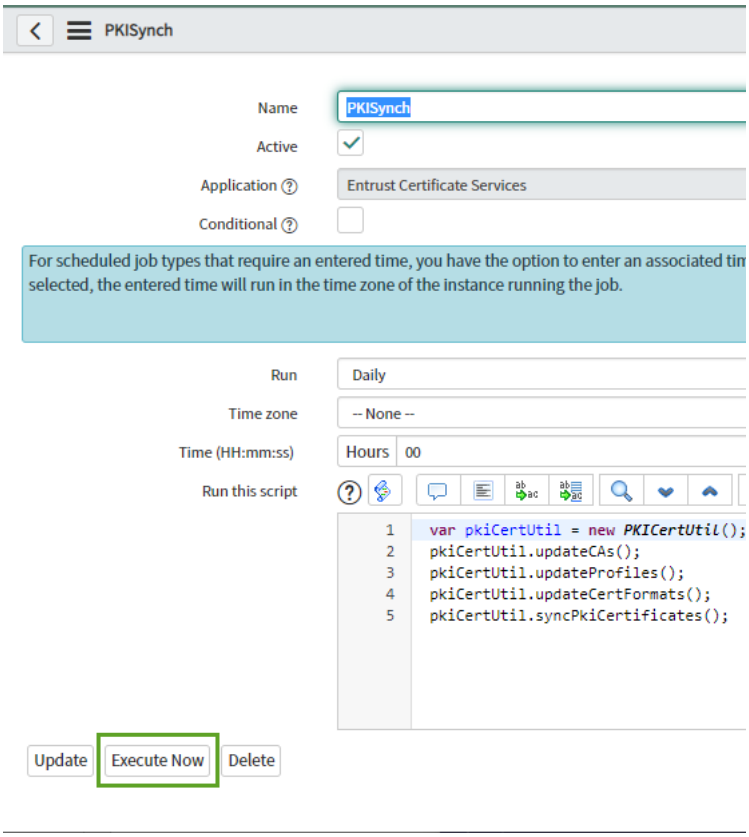
Initialize the CA and profile lists

This procedure populates the tables that store the list of CAs.

1. In the menu, select **System definition** > **Scheduled Jobs**.
2. Search for **PKISynch**.



3. Open the *PKISynch* job and click **Execute Now**.



Create Certificate Manager 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.

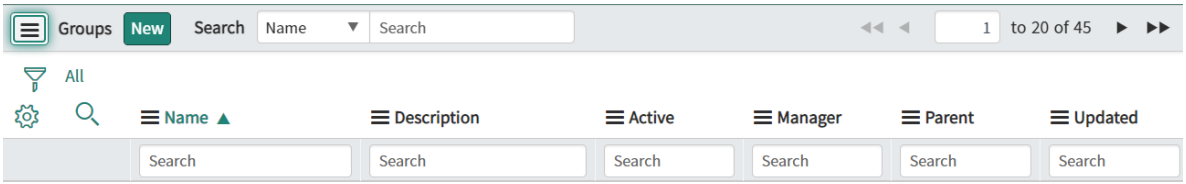
The Entrust Certificate Manager for ServiceNow is designed to have the following groups.

- 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.
- Optionally, you can create the approver user group. Approvers can approve certificate requests.

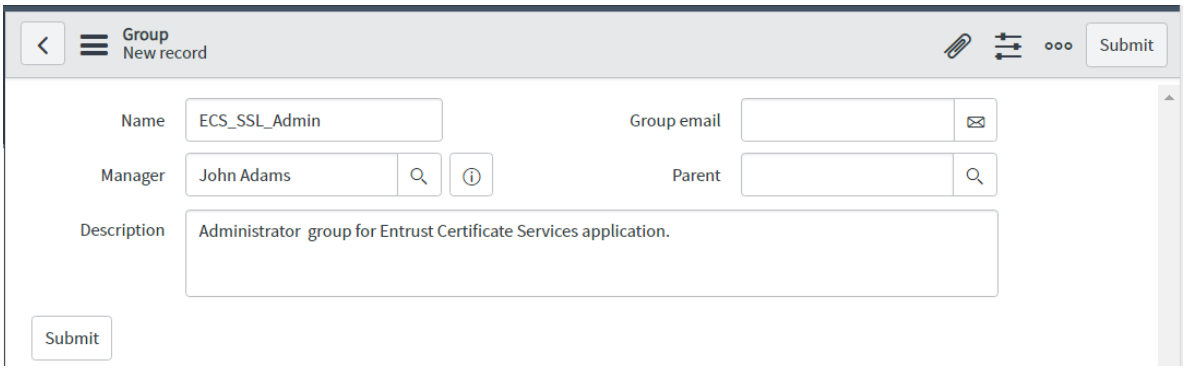
To create user groups

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

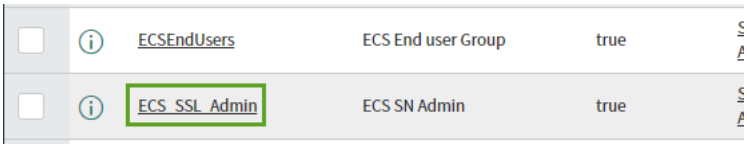
2. Click **New** to create a new group.



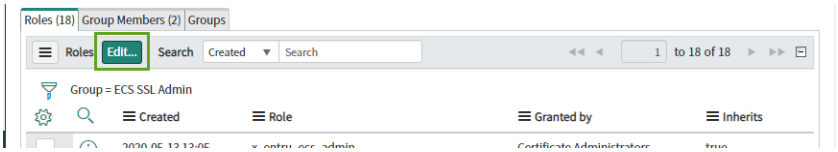
3. Enter a name for the group, group manager, and email address to receive notifications about the group. Add a meaningful description for the group.



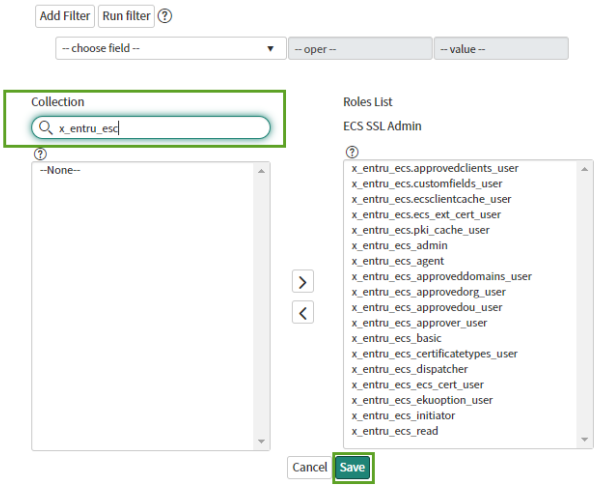
4. Click **Submit**.
5. In the Groups page, add the roles associated with each group:
   a. Click one of the groups that you created: this procedure uses the administrator group.



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



   c. To find the Certificate Services roles, enter `x_entru_esc` 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**.

4. Repeat this procedure for 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
5. Optionally, repeat the procedure for the approver user group, giving it the following role only:
   - x_entru_ecs_approver_user

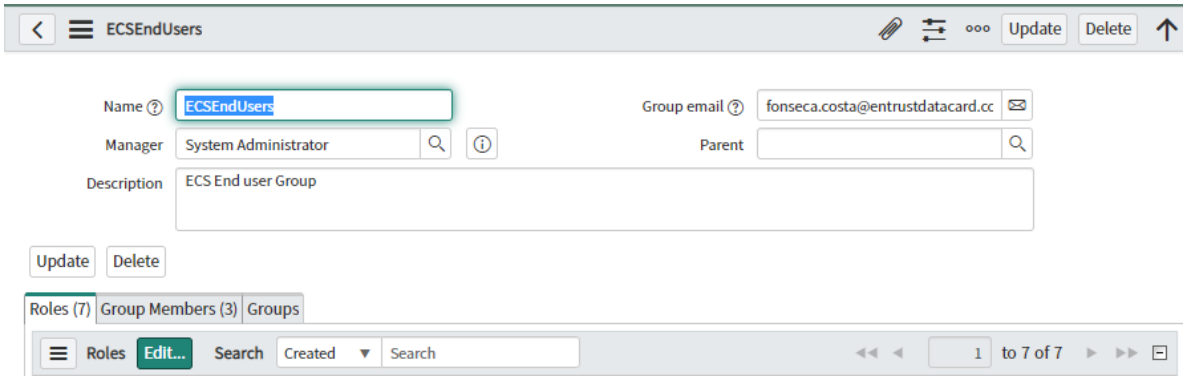
Assign users to your groups as outlined in the following procedure.

To assign users to Entrust Certificate Manager roles

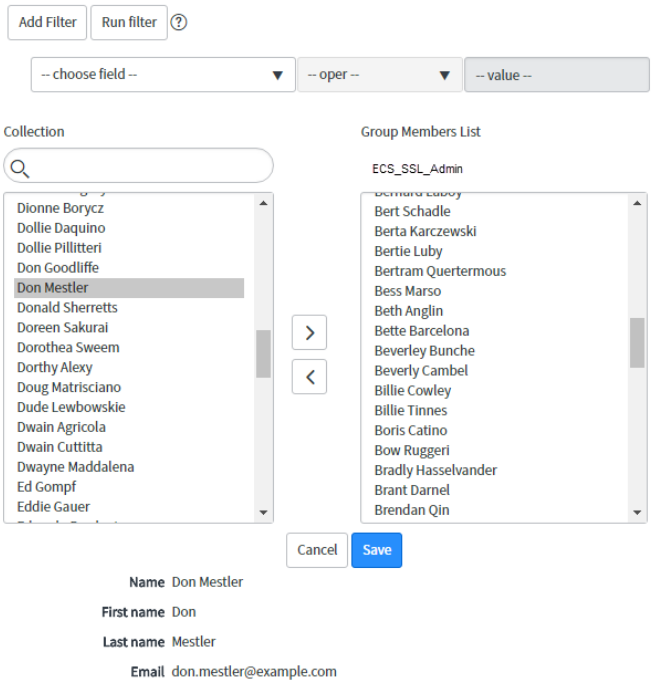
1. Navigate to System Security > Users and Groups > Groups.

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, adding users to the other Certificate Services groups.
6. Click **Save**.
7. If you are configuring the CMDB functionality, proceed to the section Using CMDB. If you are configuring Domain separation go to the section

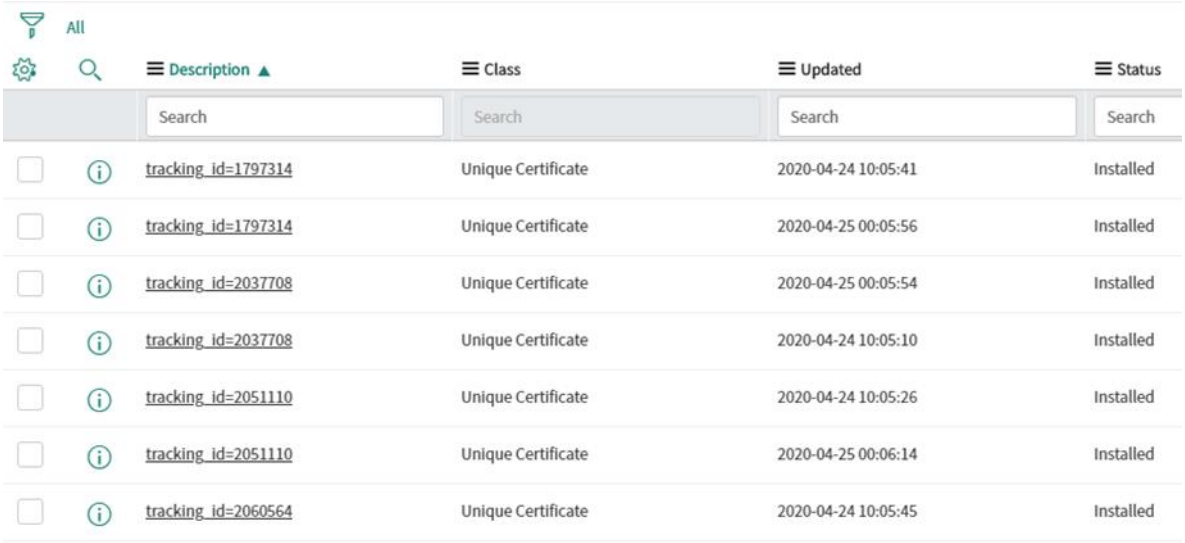
Domain separation. If you are not configuring either CMDB or Domain Separation go to the section, Initialize the database.

Using CMDB

If you chose to install the CMDB plugins and application as outlined in Prerequisites for CMDB functionality each issued ECS SSL or PKI certificate creates a corresponding CMDB CI Certificate record.

To correlate ECS SSL and PKI certificates with their respective records in CMDB, the 'Description field' of the CMDB CI Certificate record will contain:

- for the ECS SSL certificates: **tracking_id**= and the ECS certificate tracking id
- for the PKI certificates: **serial_number**= and the PKI certificate serial number

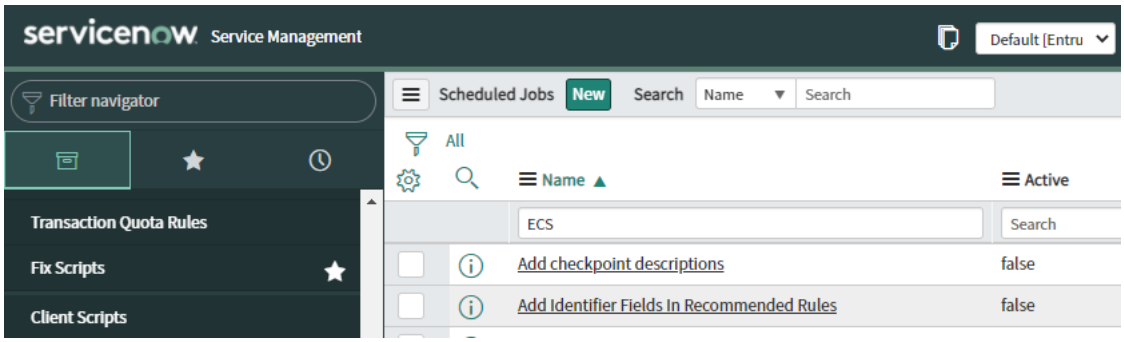


When an ECS SSL or PKI certificate is revoked or renewed, it is automatically deleted from Certificates table, and its CMDB CI certificate status is set to *Retired*.

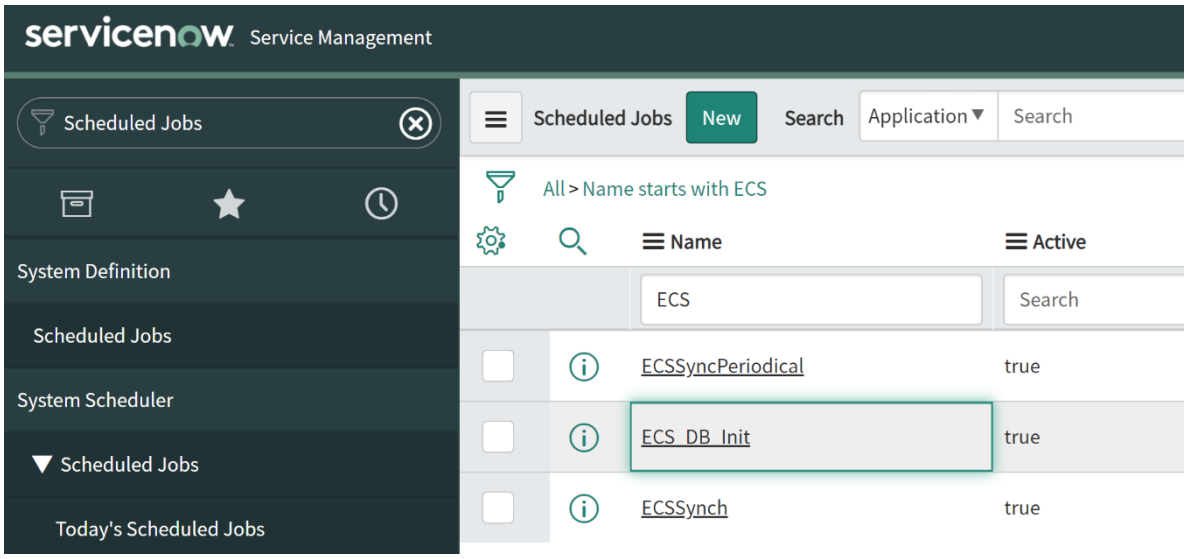
If you are configuring Domain Separation go to Domain separation, if you are not configuring domain separation proceed to Initialize the database.

Initialize the database

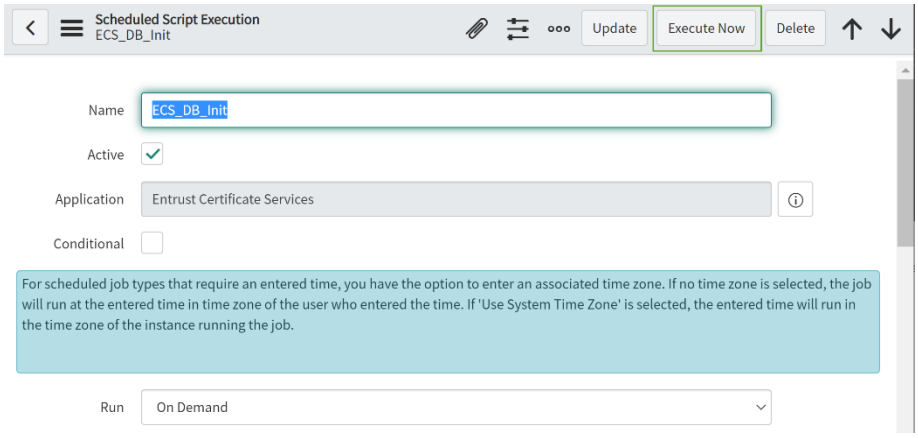
1. Navigate to System Definition > Scheduled Jobs. For example, search on Scheduled Jobs.
2. Click the magnifying glass icon, to expand the **Search** fields under the column headings. Enter ECS in the **Name** column search box.



3. Click ECS_DB_Init to initialize the application database records.



4. In the ECS_DB_Init scheduled script page, click **Execute Now**.



5. Log out and close the browser. Log in again.

This completes the installation. For information about using obtaining and managing Entrust certificates using ServiceNow, see the *Entrust Certificate Manager for ServiceNow User Guide*.

Domain separation (optional)

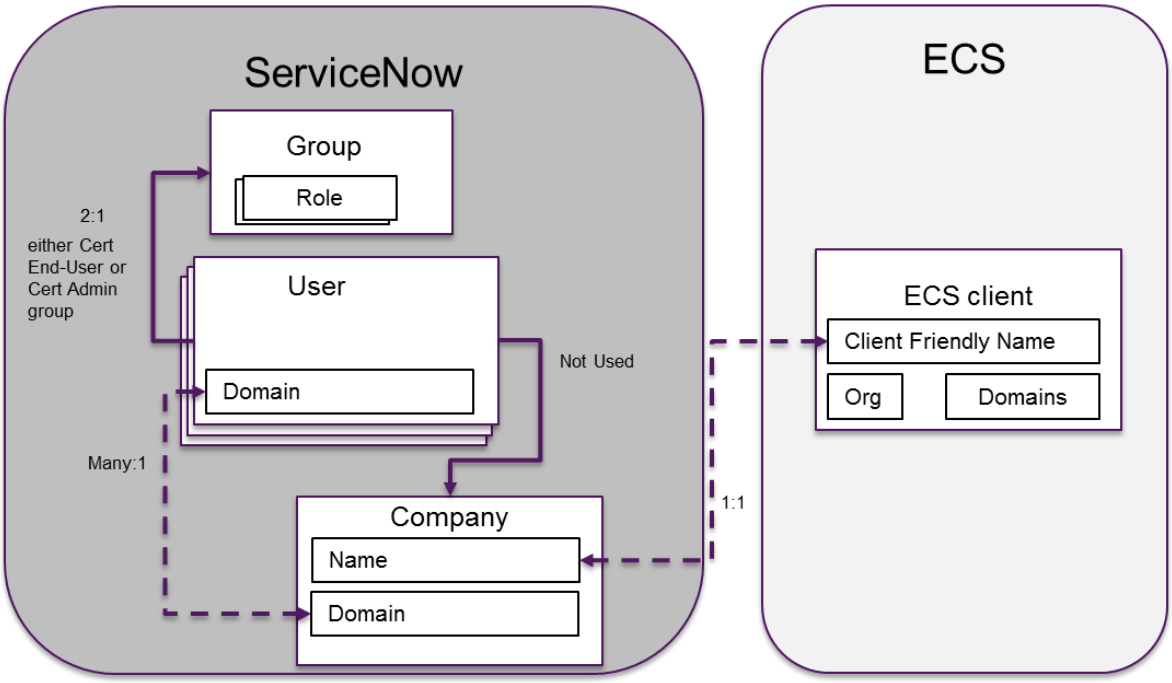
Domain separation is a ServiceNow platform feature that allows you to separate data for different groups of users in a ServiceNow instance. The Entrust Certificate Manager for ServiceNow is domain separation aware with support for Level 1 – Tenant data management as defined in the ServiceNow domain separation model.

Support for domain separation in the Entrust Certificate Manager for ServiceNow is primarily intended to support Managed Service Provider (MSP) use cases. In the Entrust version of the MSP model there are three classes of domain:

- *Global* domains are visible to the all Entrust Certificate Manager for ServiceNow users and administrators.
- Individual end-customer domains are visible to the end-customer's users and administrators (assuming that users and administrators are assigned to the end-customer's domain). These are typically identified by domain names such as *TOP/MSP/CustomerName*.
- The *Default* domain is only visible to the System Administrator. If the Entrust Certificate Manager receives information from the Entrust Certificate Services API that it cannot identify with an end-customer domain, the information is stored in the Default domain.

Each domain that an end-customer will use to issue certificates through the Entrust Certificate Manager must have a corresponding *Client* created in the MSP's Entrust Certificate Services portal account. A Client is an entity created within an ECS account for the purpose of issuing certificates for the organization. Clients own one or more top-level DNS domains (such as entrust.com or entrust.net).

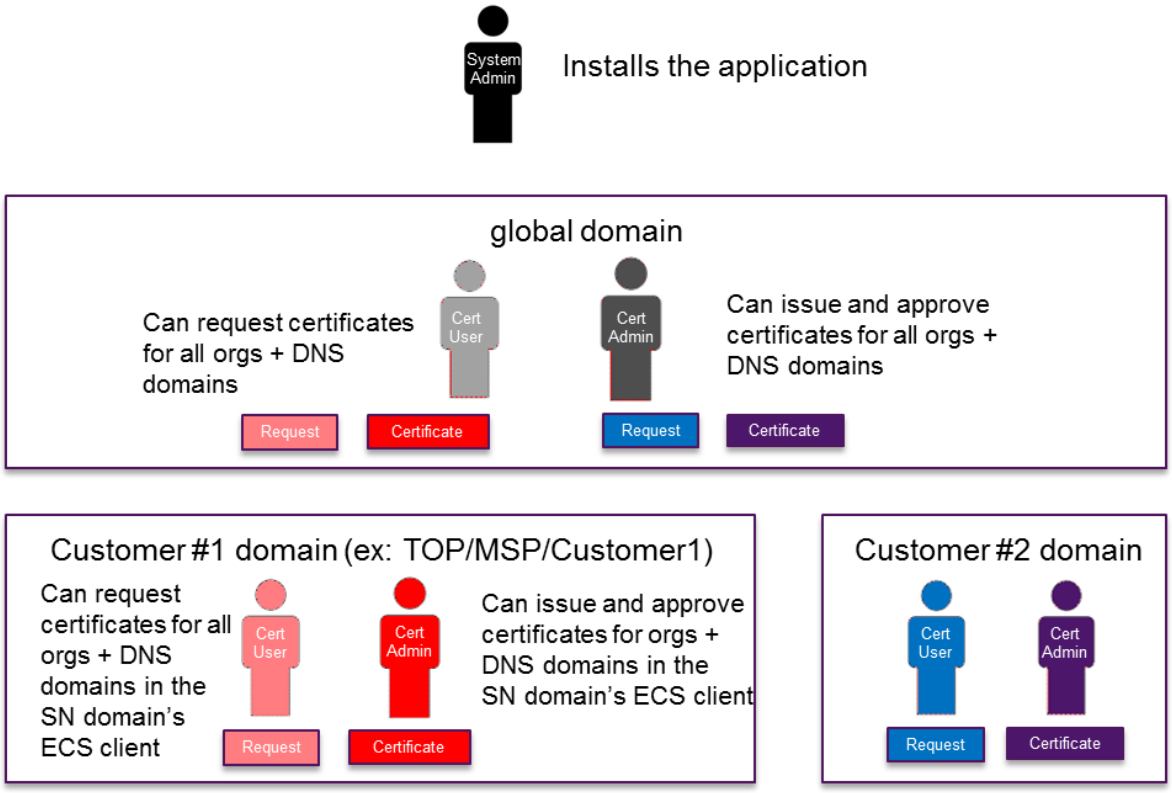
The Client is linked to the end-customer's ServiceNow domain by the *Company* configured for the end-user in ServiceNow.



The *Client Friendly Name* assigned to the Client in Entrust Certificate Services must match the name of a Company in ServiceNow. The Company in ServiceNow must be assigned to a domain in ServiceNow to complete the association of the Entrust Certificate Services Client to the ServiceNow domain.

Three types of user interact with the Entrust Certificate Manager for ServiceNow:

- System Administrator – The person (or persons) who downloads the application from the ServiceNow Store and performs the installation steps.
- Certificate Administrators – The persons who have permission to:
  - issue certificates without approval
  - approve certificate requests from Certificate End Users
  - view certificates issued to Organizations that are visible in their assigned domain
- Certificate End Users – The persons who have permission to:
  - request certificates for the Organizations accessible to their ServiceNow domain
  - view certificates assigned to themselves



The ServiceNow group to which a user is assigned will determine the role the user will assume:

- Members of the *ECS_SSL_Admin* group have the ability to issue certificates and approve certificate requests for the organization or organizations assigned to their domain.
- Members of the *ECS_SSL_EndUser* group have the ability to request certificates for the organization or organizations assigned to their domain.

Enabling domain separation for your instance

The company that requested the Entrust Certificate Services account in the Entrust portal is the *Primary Client* for the account. If you obtain and manage certificates for other companies or organizations, you add them to your account as (non-primary) Clients. The following procedures in ServiceNow should be performed for the Primary Client and non-primary Clients.

> **Attention**: Be sure to map your primary client in Entrust Certificate Services to the MSP domain in ServiceNow and each of your non-primary ECS clients to a company (domain) in ServiceNow. Any data received by ServiceNow that is not assigned to a specific domain is placed in the Default domain.

To move data from Default to the correct domain, either:

- Configure (or correct) the mapping for the client/domain. The nightly update of the Entrust Certificate Manager database will then place the data in the correct domain.
- Configure (or correct) the mapping for the client/domain and as system administrator, reinitialize the database manually. This avoids a delay while waiting for the nightly update.
- Move individual certificate data manually by changing the domain listed on the certificate grid using the drop-down list.

To enable Domain Separation support in your ServiceNow instance

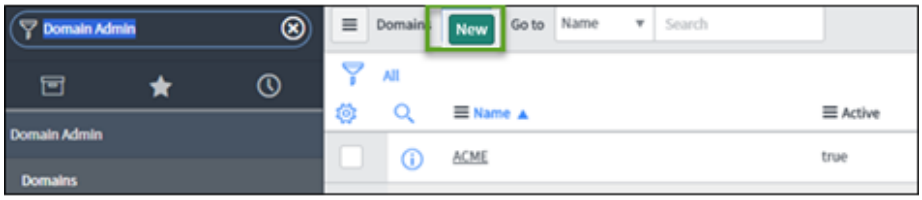
1. If domain separation is not installed in your ServiceNow instance, contact your ServiceNow representative and have the *Domain Support—Domain Extensions Installer* plugin added to your ServiceNow instance or request the service from the ServiceNow Hi portal. Receiving the service may take a day or two.

   For more information about domain separation in ServiceNow, see the ServiceNow documentation.

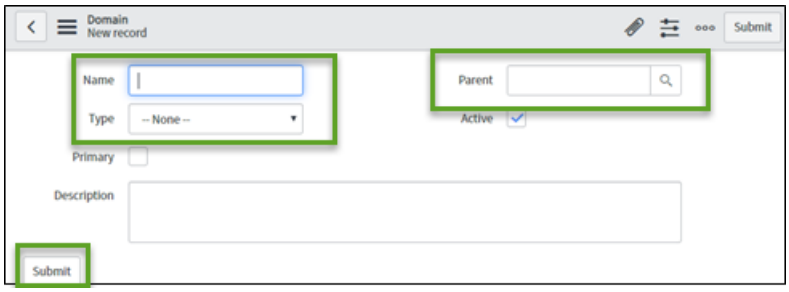
To configure a new End Customer

1. Create a domain that corresponds to the End Customer being configured (if you have not done so).

   f. Navigate to **Domain Admin** > **Domains** and click **New**.



   g. In the Domain page:

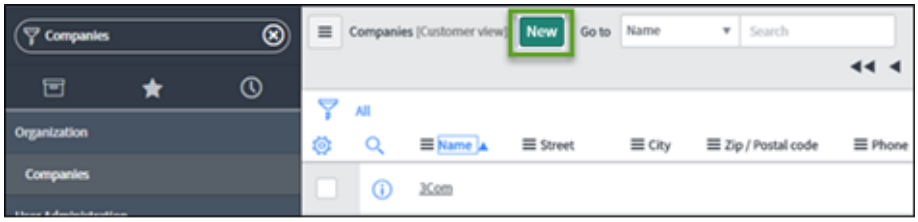


- Enter the name you have chosen for the domain.
- Select the type of domain (typically the Customer type).
- Enter the parent domain (the top level domain that contains all customer domains).
- Optionally, enter a description of the domain.

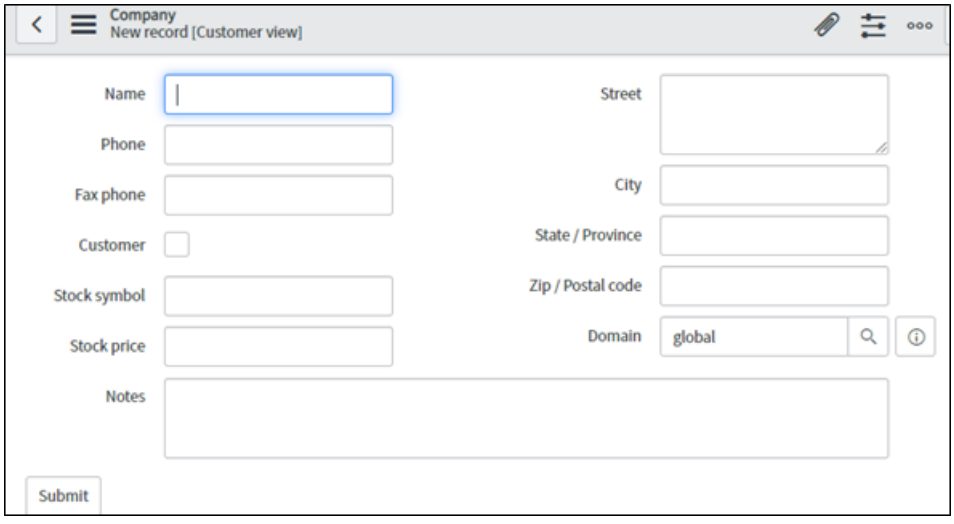
h. Click **Submit**.

2. Add a company in ServiceNow that corresponds to the End Customer being configured.

   a. Navigate to **Organizations** > **Companies** and click **New**.



   b. Fill in the company information. The domain should be the same as the one created in Step 1. The name of the Company must be the same as the Client Friendly Name of the Client in Entrust Certificate Services.

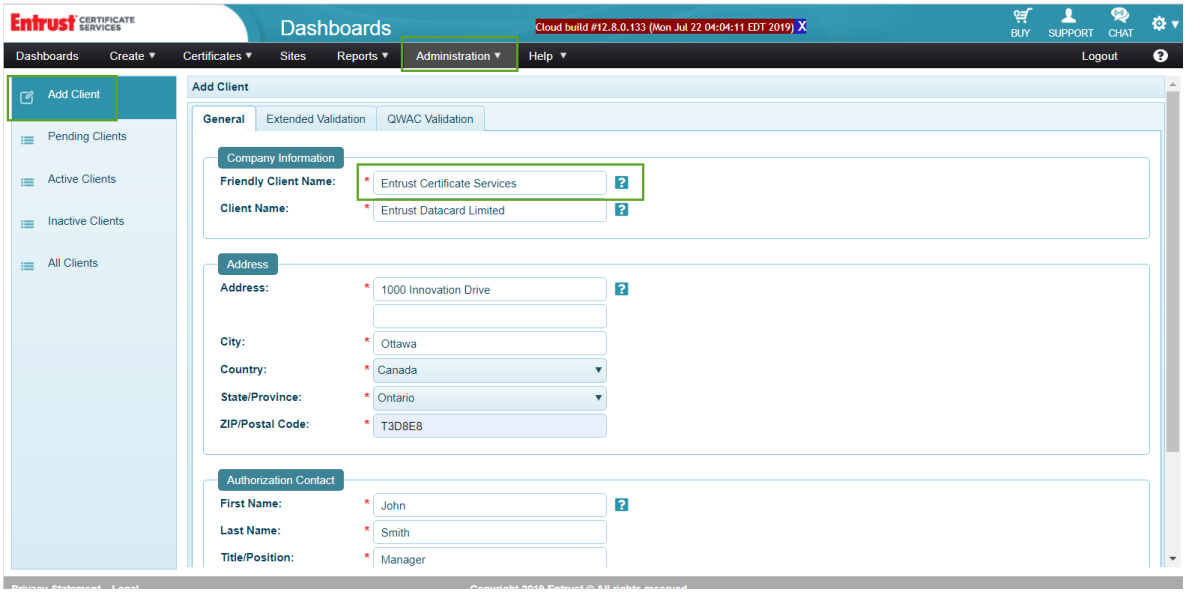


c. Click **Submit**.

3. In the Entrust Certificate Services portal, create a Client that corresponds to the End Customer.

   a. In the Entrust Certificate Services portal, navigate to **Administration** > **Client Management**.

   b. Click Add Client.



- Fill in the form. The **Client Friendly Name** must exactly match the company name In ServiceNow. If you have any difficulty filling in the form consult the online help.

  c. Click **Submit**.

- Entrust contacts the authorization contact. When the information in the form has been verified, the Client is available for use.

To synchronize the data between ServiceNow and Entrust Certificate Services

To synchronize the data between ServiceNow and Entrust Certificate Services, initialize the database, as explained in the section Initialize the database.

To configure a new End Customer user

1) Create the User in ServiceNow as usual.
2) Assign the user to a Company in ServiceNow that corresponds to the End Customer.
3) Assign the user to same domain as the Company of which they are a member.

> The Company must have the domain configured appropriately as Entrust Certificate Manager for ServiceNow looks at the Company's domain rather than the user's domain.

4) Assign the user to the ECS_SSL group that matches their role (see Create Certificate Services user groups and assign users.