Entrust Certificate Manager for ServiceNow

User Guide

Document issue: 2.3

Date of issue: May 2022

Contents

Contents 3
Audience and guide information 4
Audience 4
Viewing this guide 4
Conventions 4
ServiceNow version 4
Contacting support 4
Introduction 5
Before you begin 5
Roles and privileges 5
Types of certificates 6
Generating a certificate 7
To generate a certificate 7
To generate a PKI certificate 11
Viewing certificate requests 14
Approving certificates 16
To approve a certificate 16
CMDB CI Certificate 17
To display the CMDB CI certificates 17
Downloading your SSL/TLS certificate 19
To download a certificate 19
To download a certificate 21
Renewing a certificate 22
To renew a certificate 22

Audience and guide information

Audience

This guide is intended for Entrust Certificate Services Enterprise portal or Entrust CA Gateway users who want to generate and renew certificates through their ServiceNow account. This guide assumes that the user is familiar with both ServiceNow and Entrust Certificate Services Enterprise and/or CA Gateway and can has been assigned the appropriate role.

Viewing this guide

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

Conventions

- *ECS* or *Entrust 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 to refer to the **Entrust CA Gateway** configuration

ServiceNow version

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

Contacting support

If you experience an issue with the Entrust Certificate Manager for the ServiceNow application, contact Entrust Support by clicking **Entrust Support** in the Entrust Certificate Manager for ServiceNow menu. For ServiceNow issues contact ServiceNow support.

Introduction

Entrust Certificate Manager for ServiceNow allows:

- ServiceNow users with a PKI account (using Entrust CA Gateway) to generate Entrust PKI certificates.
- ServiceNow users with an Entrust Certificate Services pooling account to generate or renew Entrust SSL/TLS certificates from the ServiceNow application.
- Employ CMDB functionality.

  Attention: This application does not support the Entrust Certificate Services Enterprise certificate pickup password feature. Disable the password feature in your Entrust Certificate Services Enterprise portal account..

Before you begin

The following are required to use this application:

- To use the Entrust Certificate Manager for ServiceNow, you must have an Entrust Certificate Services Enterprise *pooling* account.
- The Entrust Certificate Manager for ServiceNow application is available from the ServiceNow App Store. To install the application, you must have ServiceNow administrator privileges. Installation and configuration instructions are available in the *Entrust Certificate Manager for ServiceNow Installation Guide.*

  Note: Select the favorites icon () beside the **Entrust Certificate Services** menu entry to add Entrust Certificate Manager for ServiceNow to your **Favorite** tab.

Roles and privileges

The Entrust Certificate Manager for ServiceNow supports three user roles by default: Administrators, End Users, and Approvers.

Note: This section refers specifically to Entrust Certificate Manager for ServiceNow roles.

- Administrators can:
  - request and renew certificates without additional approval
  - approve, reject, or delete requests
  - see detailed information about certificates and requests
  - request certificates for other users

- End Users can also request and renew certificates, but their requests require administrator approval. Users see their own certificate requests or those assigned to them.
- Approvers (if approvers have been configured) can see and approve certificate requests.

  Note: *Approver* is optional role that may or may not have been configured by your ServiceNow Administrator when this application was installed.

Types of certificates

Entrust Certificate Manager for ServiceNow offers the ability to create and manage Entrust SSL/TLS certificates. For more information about these certificates, see our web site. If the PKI option was configured during installation, this application can create PKI certificates.

Entrust sells many different types of certificates, including SSL/TLS, document signing, code signing, and secure email certificates. These certificates can be purchased, generated, and managed through your Entrust Certificate Services Enterprise account.

Note: Some certificate names have changed in Entrust Certificate Services Enterprise. See the following table for more information:

Old certificate name	New certificate name
Advantage SSL	Advantage OV SSL
SANs (various names)	Extra SANs for OV Certificates Extra SANs for EV Certificates
Standard SSL	Standard OV SSL
UC Multi-Domain SSL	Multi-Domain OV SSL
Extended Validation Multi-domain SSL	Multi-Domain EV SSL
Wildcard SSL	Wildcard OV SSL

Generating a certificate

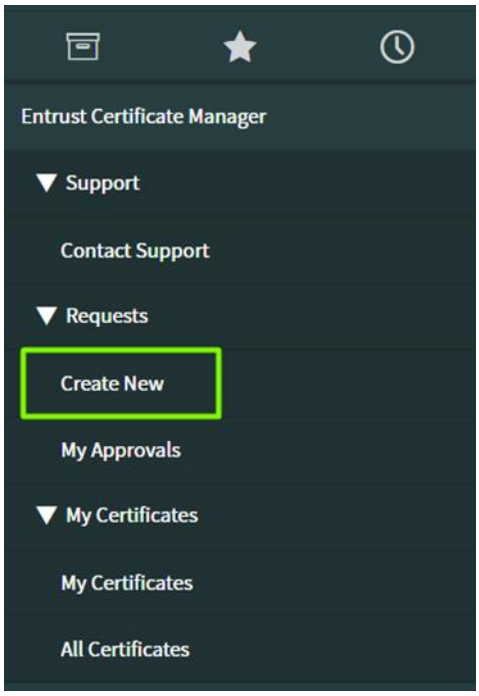
To generate a certificate, you require a Certificate Signing Request (CSR). A good security practice is to create the CSR on the server where you will install the certificate. By doing so, you generate and store the private key in place.

The tool you use to create the CSR depends, in part, on the type of server where you are installing the certificate—for example, keytool is commonly used on Java-based web servers and OpenSSL is often used on Apache-based web servers. The Entrust Certificate Services knowledge base offers specific information about creating CSRs for various servers.

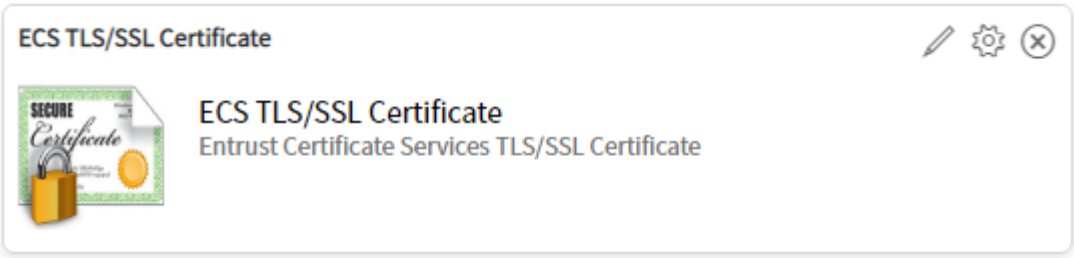
If you are generating certificates from Entrust Certificate Services Account where the CA Gateway is used, the user requesting the certificate (owner) must have their corporate email address, and telephone number included in their user information. If any of these are missing, the Entrust Certificate Manager for ServiceNow will generate an error.

To generate a certificate

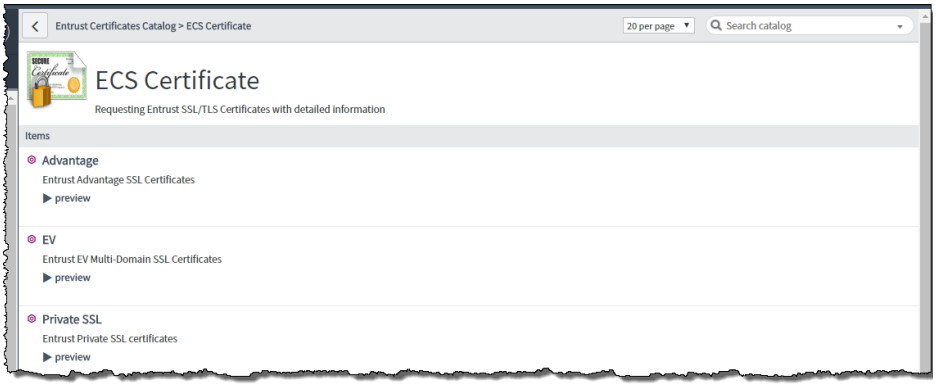
1. In the left pane, under **All applications** ( ) scroll down to **Entrust Certificate Manager**.



2. Expand **Requests** and select **Create New**.
3. Click **ECS TLS/SSL Certificate**.



4. Under **Items**, select the type of certificate you want to create. For information about a certificate type (Standard, for example), expand **preview**. For additional information about certificate types, visit our web site here.



5. In the **Owner** field, either enter the name of the certificate owner or click (search) and select an owner from the list. By default, the field is prefilled with the name of the person requesting the certificate. The certificate owner is the person who will be responsible for managing the certificate. An administrator can transfer the certificate to a different owner.

   The list contains the names of all of the Entrust Certificate Services application users. If you enter a name manually, it must match a name in the list or the application generates an error.

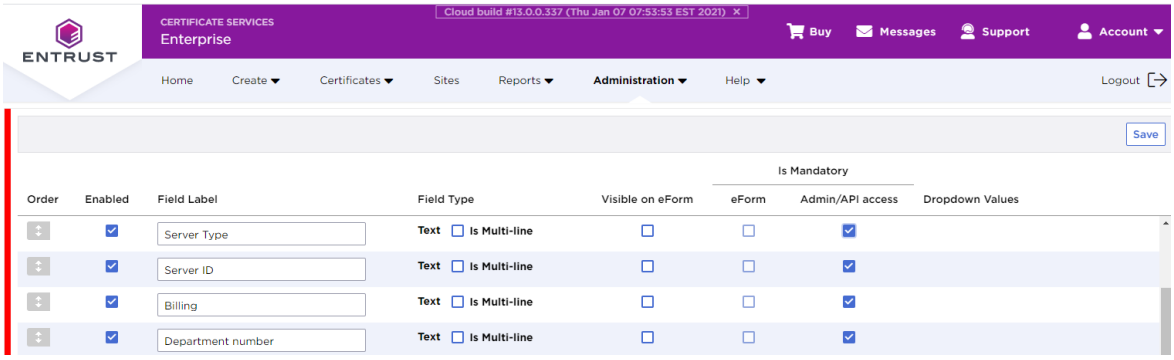
6. Select an **Expiry Date**. Publicly rooted certificates must have a minimum life span of 60 days and maximum lifespan of 13 months. Privately rooted certificates can have a life span of between 60 days and 39 months.
7. In the **CSR** field, paste the Certificate Signing Request created for the certificate. Be sure to include the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- lines.
8. In the **Organization** field, select a valid organization from the pull-down menu.

Note: If your instance uses the Domain Separation feature, the pull-down menu displays only organizations and organizational units that are associated with the current user's domain.

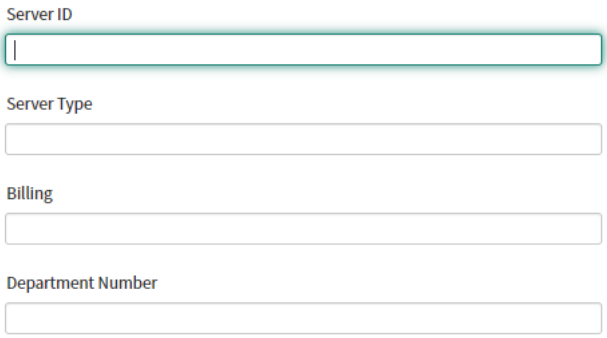
9. In the **Organizational Unit** (OU) field, select a valid OU from the pull-down menu.
10. In the **Subject Alternative Name** (SAN) field, enter or paste a comma-separated list of additional domains to add to the certificate. Most Entrust SSL/TLS certificate types permit you to include a limited number of domains for free. Additional domains consume SAN licenses from your account.

    The maximum number of additional domains permitted depends on the type of certificate.
11. From the **Extended Key Usage** pull-down menu, select the type of authentication required—**ClientAuth** (Client Authentication), **ServerAuth** (Server Authentication), or **ServerAndClientAuth** (Server and Client Authentication). If you are not sure, select **ServerAndClientAuth**.
12. Enter the information for the Tracking Fields that you configured in your Entrust Certificate Services Enterprise portal account. You must include fields marked as *Admin/API Access.* Only fields that are enabled appear in the form.

Tracking Fields (Entrust Certificate Services Enterprise)

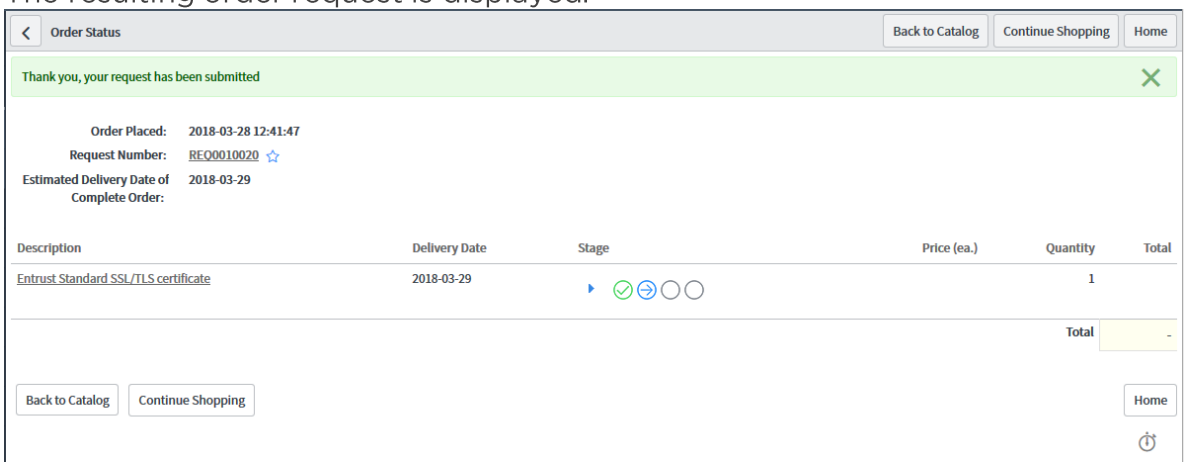


Tracking Fields (Entrust Certificate Manager for ServiceNow)



13. Click **Add to cart** if you intend to create additional certificates or **Order Now** to complete your request. If you use the cart, click **Proceed to checkout** when you have finished.

    The resulting order request is displayed.



Note: Orders created by Administrators do not require approval and bypass the request stage. These certificates are created immediately.

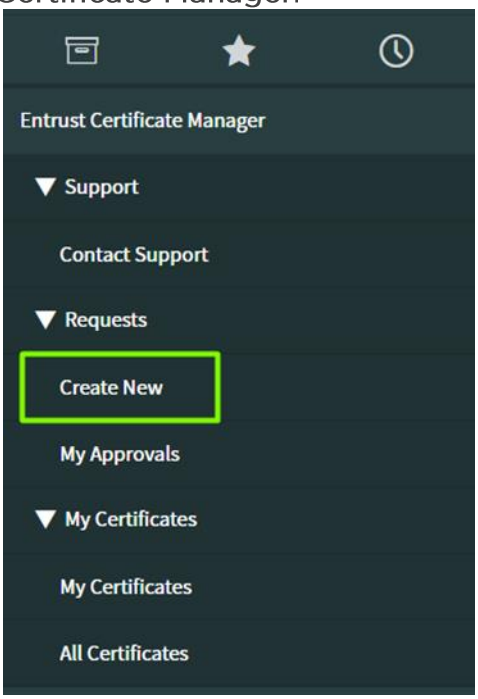
Use the link in the **Request Number** field to open a page where you can check the contents of the order. The link in the **Description** column opens a page where you can check and edit certificate request information. The abbreviations used in the **Item** field on this page are:

Abbreviation	Name used in ServiceNow
standard	Standard SSL Certificate
advantage	Advantage SSL Certificate

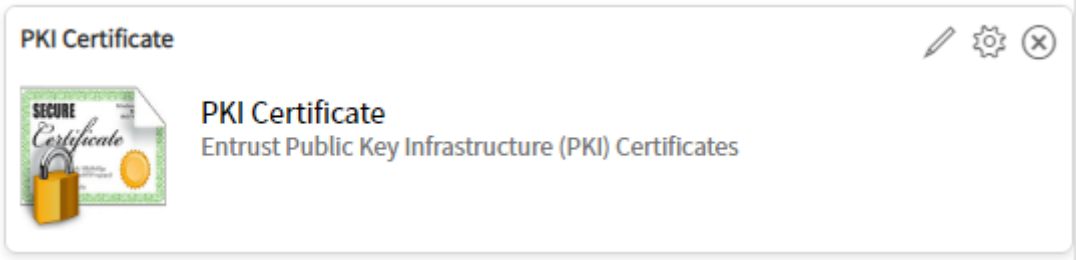
ev	Extended Validation Multi-Domain SSL Certificate
ucc	Unified Communication Multi-Domain SSL Certificate
wc	Wildcard SSL Certificate
ic	Private SSL Certificate

To generate a PKI certificate

1. In the left pane, under **All applications** ( ) scroll down to **Entrust Certificate Manager**.



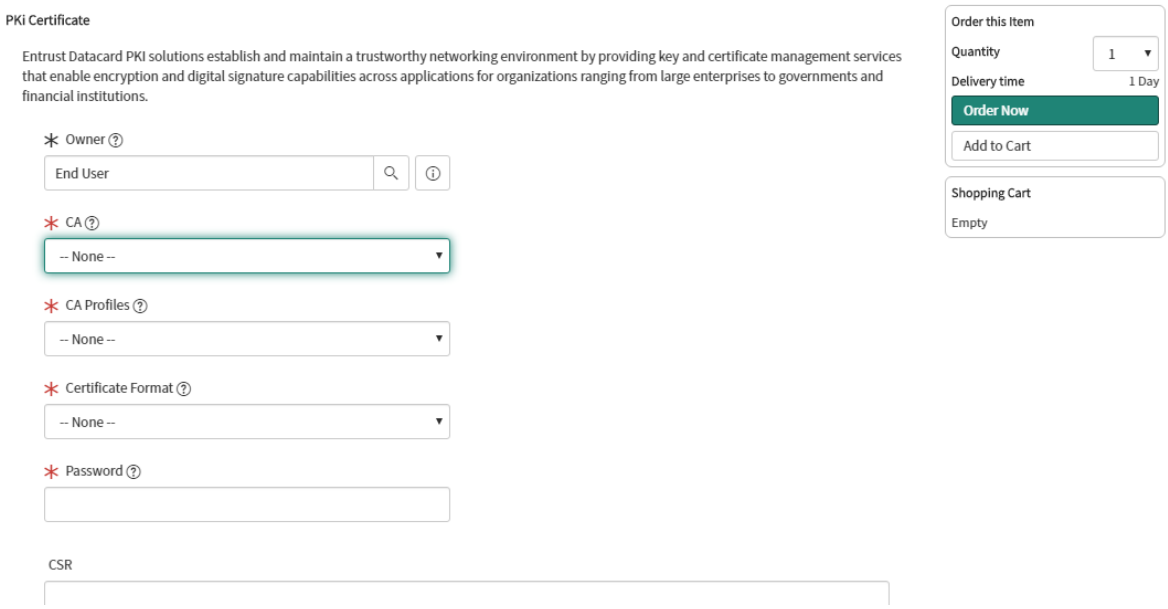
2. Expand **Requests** and select **Create New**.
3. Click **PKI Certificate**.



4. Under **Items**, select **Order PKI Certificate**

5. In the **Owner** field, either enter the name of the certificate owner or click (search) and select an owner from the list of Entrust Certificate Manager for ServiceNow users. By default, the field is prefilled with the name of the person requesting the certificate.

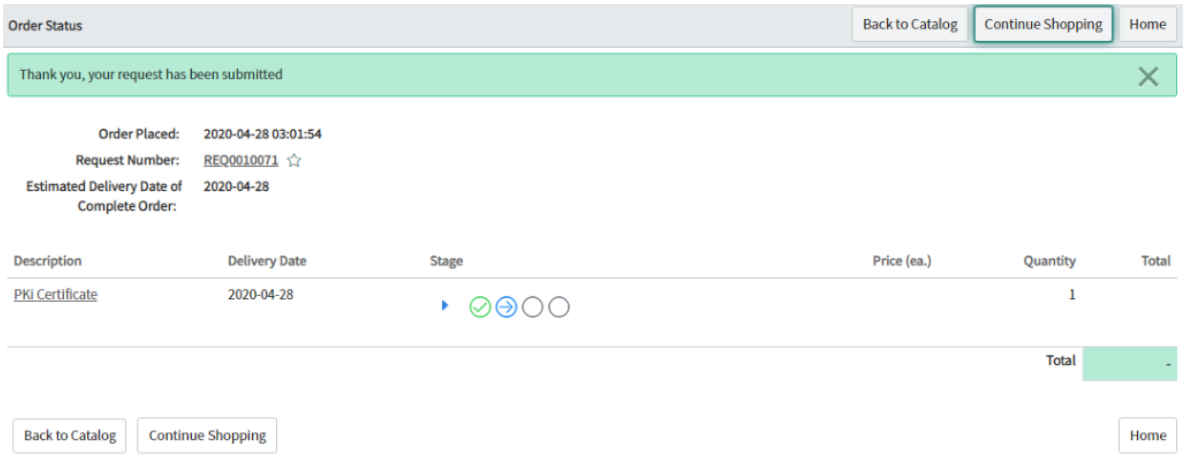
   The certificate owner is the person who will be responsible for managing the certificate. An administrator can transfer ownership of the certificate to a different user.



6. In the **CA** field, select the appropriate Certificate Authority from the dropdown list. This will determine which CA profiles appear in the **CA Profile** list.
7. Select the appropriate profile from the **CA Profile** dropdown list
8. Select the **Certificate Format** from the options provided: **PEM**, **DER**, or **PKCS12**.
9. If you have not provided a **CSR**, enter a password for the certificate.
10. Depending on which CA Profile you selected, some of following fields are displayed:
    Common Name, Organization Unit, Organization, Company, First Name, Last Name, IP Address, Rfc822Name (email address), Other Name, Directory Name, Registered ID, Uniform Resource Identifier (URI), DNS Name.
11. Paste the certificate signing request (CSR) for the certificate into the **CSR** field. Be sure to include the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- lines.

12. In the **Validity Period** field enter an expiry date for the certificate. Click the calendar icon to use the date picker to select the date.
13. Click **Add to cart** if you intend to create additional certificates or **Order Now** to complete your request. If you use the cart, click **Proceed to checkout** when you are done.

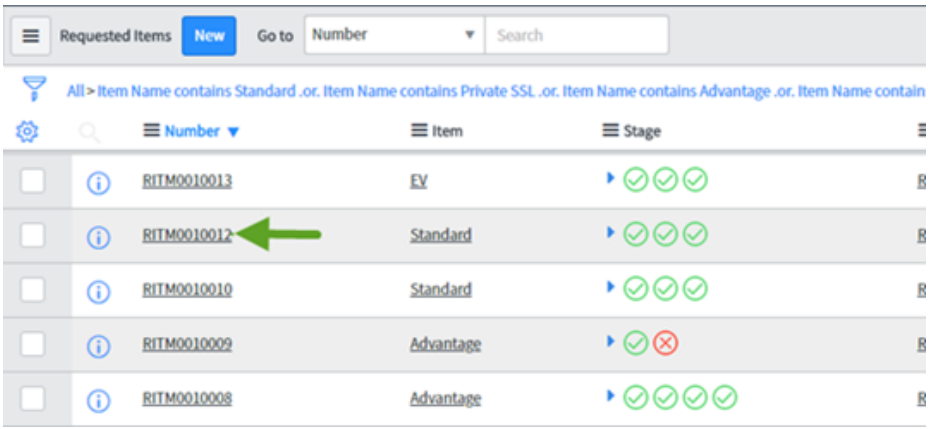
    The resulting order request is displayed.



Note: Orders created by administrators do not require approval and bypass the request stage. These certificates are created immediately.

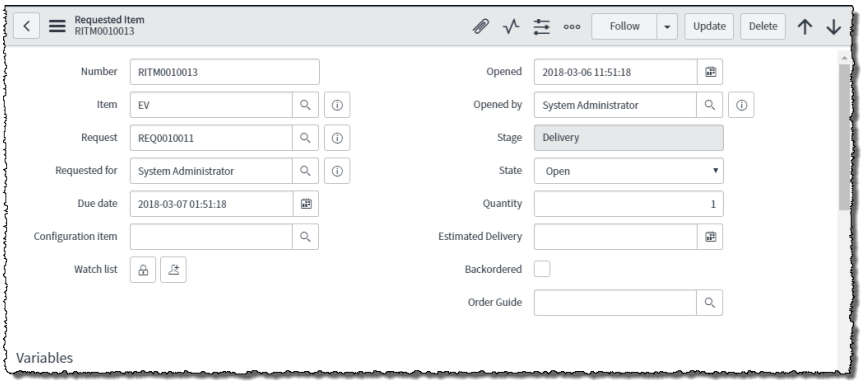
Viewing certificate requests

Select **Requests** > **All Certificates Requests** to see a grid displaying all of the current requests. To view detailed information about a request click the value in the **Number** column.



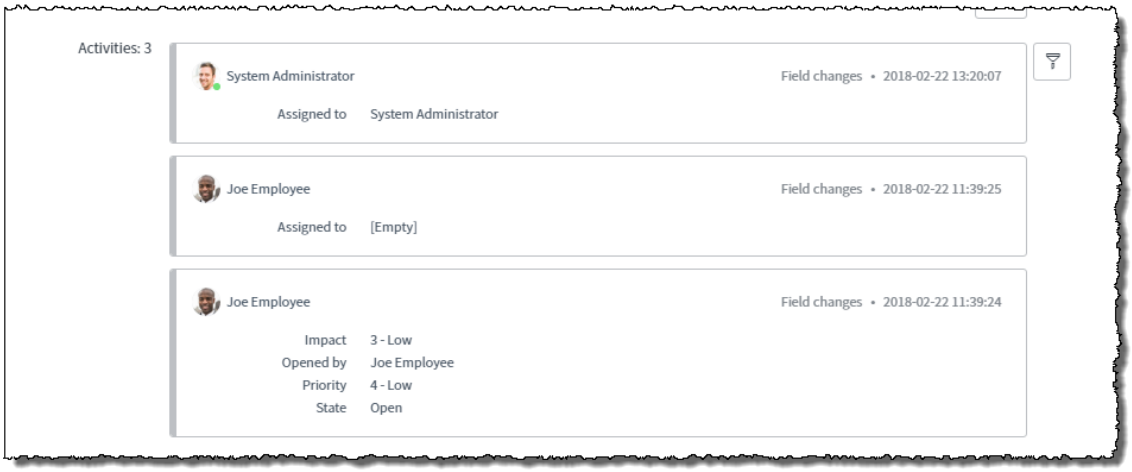
You can update some fields from this view.

Note: Not all of the fields in this page apply to the Entrust Certificate Manager for ServiceNow application.



Note: If a certificate request has failed, changing the incorrect field and clicking **Update** changes the record but does not submit a valid request.

A record of the certificate creation and any subsequent changes appears on the page.


Activities: 3
System Administrator
Field changes • 2018-02-22 13:20:07
Assigned to
System Administrator
Joe Employee
Field changes • 2018-02-22 11:39:25
Assigned to
[Empty]
Joe Employee
Field changes • 2018-02-22 11:39:24
Impact
3 - Low
Opened by
Joe Employee
Priority
4 - Low
State
Open

Approving certificates

If an administrator creates a certificate request, it does not require approval. If an end user creates a certificate request, an administrator must approve it before the transaction can be completed. A person with the certificate approver role can approve end user certificates if your administrator added the role.

Symbols in the **Stage** column indicate where the certificate is in the approval process. The icon indicates that it is waiting to complete that stage. The icon indicates that it has passed a specific stage successfully. The icon indicates that the request has failed. Hover the pointer over a symbol to see the stage. The four stages are:

Request Approved – the icon indicates the request has been successfully created

Fulfilment – the icon indicates the certificate has been created

Delivery – the icon indicates the certificate has been downloaded

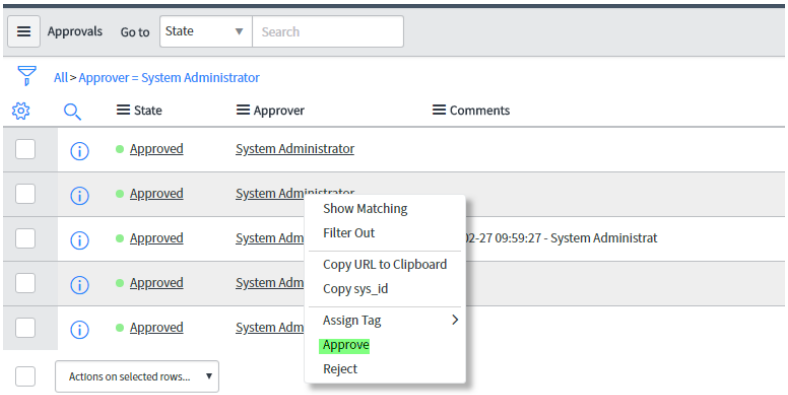
Waiting for approval – (end user requests only) the icon indicates the request has been approved by an administrator

To approve a certificate

1. Navigate to **All applications** ( ) (or the favorites tab) > **Entrust Certificate Manager** > **My Approvals**.

   If you need to review the certificate information, click (information).

2. Right-click the entry for the certificate request.
3. Select **Approve**.

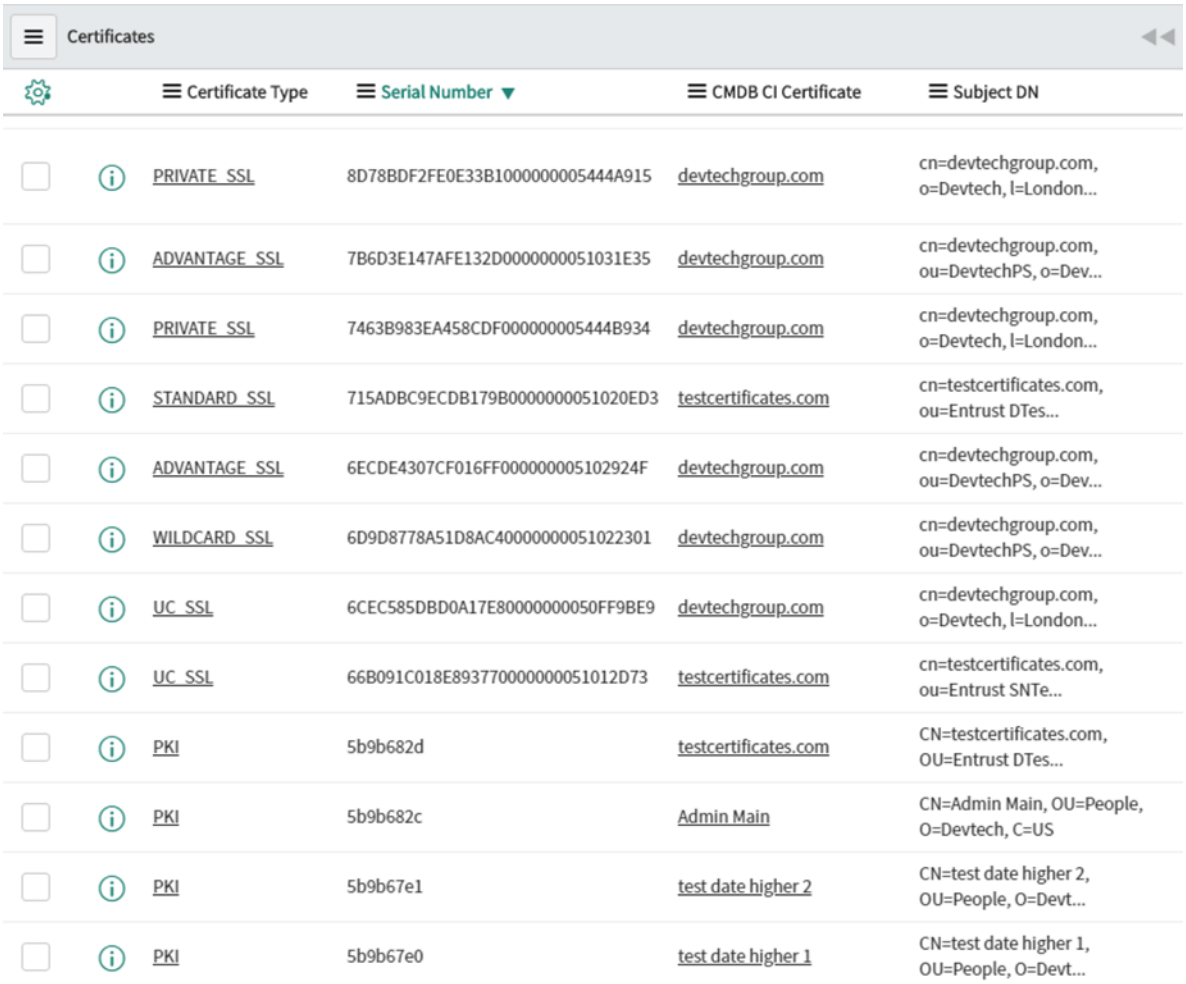


CMDB CI Certificate

If your administrator has configured CMDB (as outlined in the *Entrust Certificate Manager for ServiceNow Installation Guide)* each certificate created through either Entrust Certificate Services or the CA Gateway creates corresponding CMDB CI certificate.

To display the CMDB CI certificates

1. Navigate to **Entrust Certificate Manager** > **All Certificates.** This can be done by the end user or administrator.
2. Add the **CMDB CI Certificate** column to display these certificates.

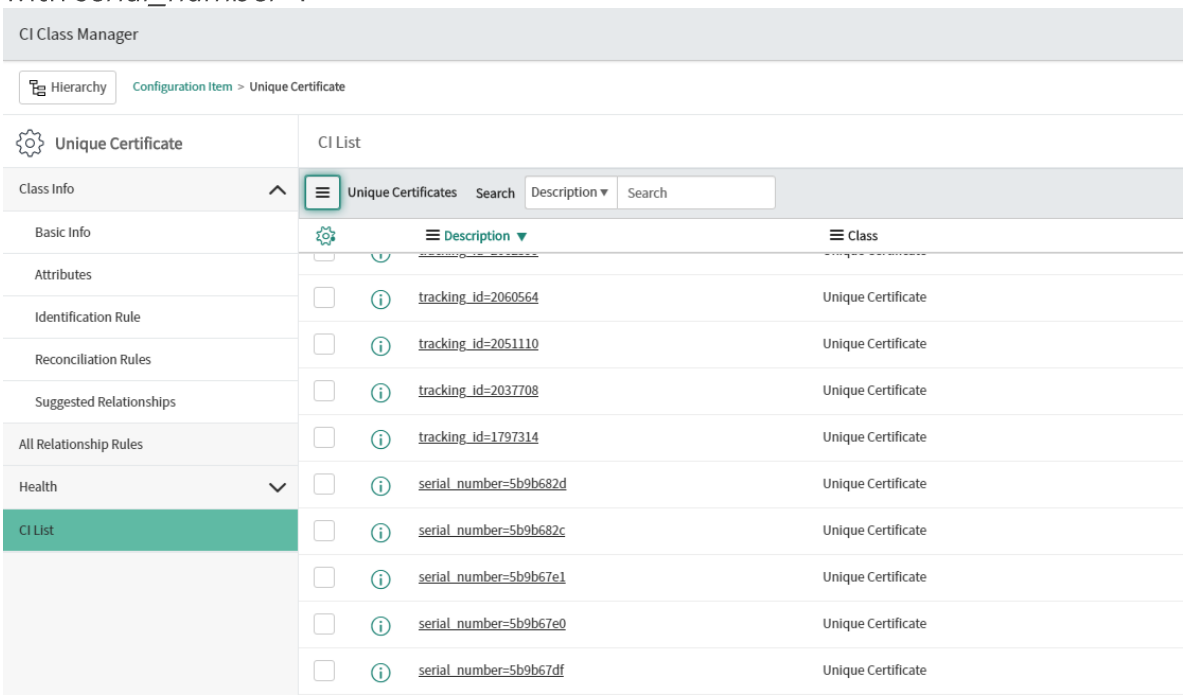


Certificates

Certificate Type	Serial Number ▼	CMDB CI Certificate	Subject DN
PRIVATE_SSL	8D78BDF2FE0E33B1000000005444A915	devtechgroup.com	cn=devtechgroup.com, o=Devtech, l=London...
ADVANTAGE_SSL	7B6D3E147AFE132D0000000051031E35	devtechgroup.com	cn=devtechgroup.com, ou=DevtechPS, o=Dev...
PRIVATE_SSL	7463B983EA458CDF000000005444B934	devtechgroup.com	cn=devtechgroup.com, o=Devtech, l=London...
STANDARD_SSL	715ADBC9ECDB179B0000000051020ED3	testcertificates.com	cn=testcertificates.com, ou=Entrust DTes...
ADVANTAGE_SSL	6ECDE4307CF016FF000000005102924F	devtechgroup.com	cn=devtechgroup.com, ou=DevtechPS, o=Dev...
WILDCARD_SSL	6D9D8778A51D8AC40000000051022301	devtechgroup.com	cn=devtechgroup.com, ou=DevtechPS, o=Dev...
UC_SSL	6CEC585DBD0A17E80000000050FF9BE9	devtechgroup.com	cn=devtechgroup.com, o=Devtech, l=London...
UC_SSL	66B091C018E8937700000000051012D73	testcertificates.com	cn=testcertificates.com, ou=Entrust SNTe...
PKI	5b9b682d	testcertificates.com	CN=testcertificates.com, OU=Entrust DTes...
PKI	5b9b682c	Admin Main	CN=Admin Main, OU=People, O=Devtech, C=US
PKI	5b9b67e1	test date higher 2	CN=test date higher 2, OU=People, O=Devt...
PKI	5b9b67e0	test date higher 1	CN=test date higher 1, OU=People, O=Devt...

3. To list all CMDB CI Certificates navigate to **CI Class Manager** > **Open Hierarchy** > search and open **Unique Certificate** > **CI List**.

The description of CMDB CI certificates for TLS/SSL certificates will begin with *tracking_id=*, PKI certificates have a short description that begins with *serial_number=*.



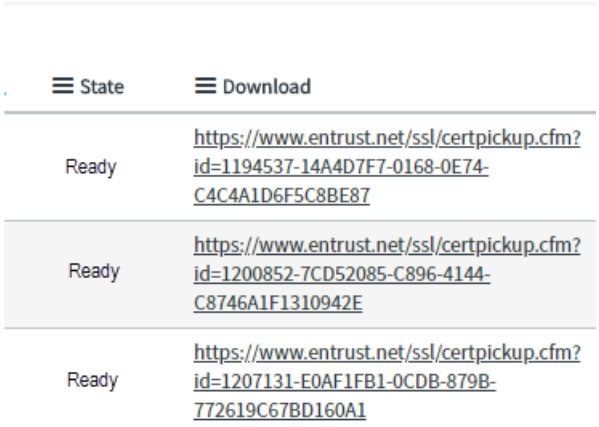
Downloading your SSL/TLS certificate

When your certificate is ready to download and install, a link appears in the **Download** column of the **My Certificates** pages. The link opens the Entrust certificate download page where you can obtain the certificate chain, including intermediate and root certificates, and an Entrust site seal for your web page.

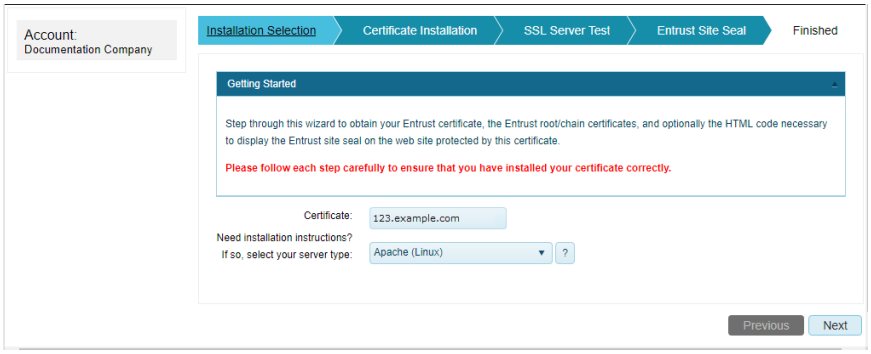
You can obtain the certificate (without the certificate chain) in PEM format from the ServiceNow details page. To open the page, select **My Certificates** > **Certificate type**.

To download a certificate

1. Navigate to **Entrust Certificate Services** > **My Certificates** > **My Certificates**.
2. Locate your certificate in the grid.
3. Follow the link in the **Download** column of your certificate.



The Entrust certificate download web pages open.



4. In the Installation Selection page:

a. In the **Certificate** field, check the domain displayed to be sure that you are downloading the correct certificate.

b. From the **What server type** [...] drop-down list, select the type of server where certificate will be installed (Apache, for example). By selecting the server, you help to ensure that you are obtaining the certificate in the correct format.

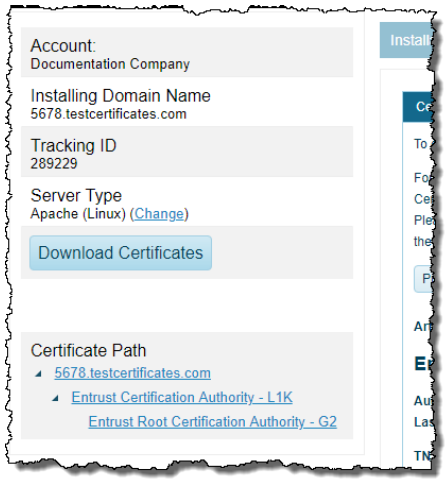
c. Click **Next**.

The Certificate Installation page appears. This page allows you to download the certificate chain or parts of the chain individually. You can also see your account name, the Domain in the DN of the certificate, and the tracking ID of the certificate (used to identify this specific certificate in Entrust Certificate Services).

5. To download the certificate, either:

   a. From the **Server Type Change** link, change the type of server if necessary.

   b. Use the **Download Certificates** button to download all certificates in the certificate chain. The file is named *<CertificateBundle>.<extension>*.



Or

   a. Select the certificates you need from the Certificate Path links. The server certificate displays the server's domain name.

   b. Instructions for installing your certificate on the type of server you specified appear on the page. Optionally, click **Print** to print them for later use.

6. Click **Next**.

7. Use the SSL Server Test link to check that the certificate is properly installed. Enter the server's domain name and click Launch SSL Server Test.
8. Click **Next**.
9. From the Site Seal page, select the Entrust site seal that is appropriate for your web site.

Downloading your PKI certificate

When your certificate is ready to download and install, a link appears in the **Download** column of the **My Certificates** page. The link downloads the certificate file to your computer.

To download a certificate

1. Navigate to **Entrust Certificate Manager** > **My Certificates** > **My Certificates**.
2. Locate your certificate in the grid.
3. Follow the link in the **Download** column of the entry.

Renewing a certificate

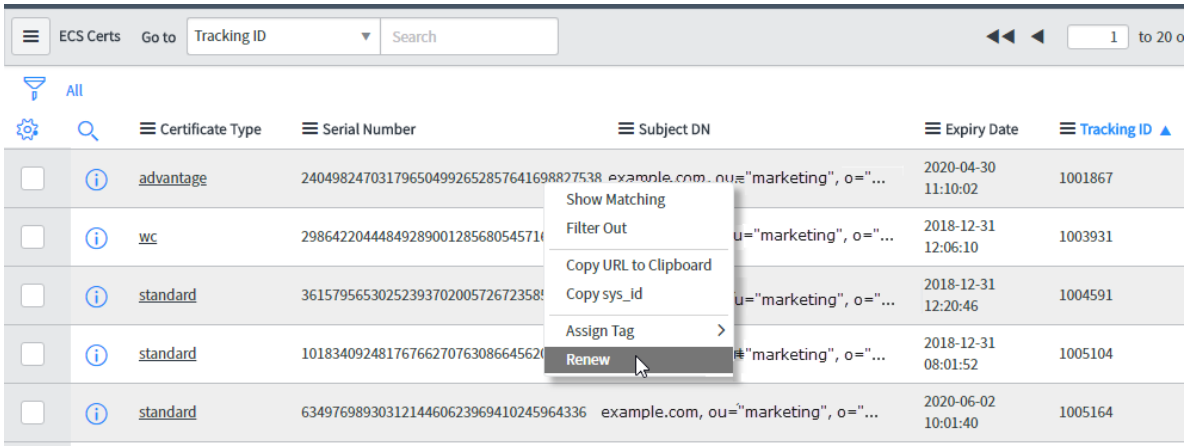
Any SSL certificate that you create from your account must be at least 30 days old before you can renew it. You can begin renewing certificates from the **My Certificates** page.

Renewal is not currently supported for PKI certificates.

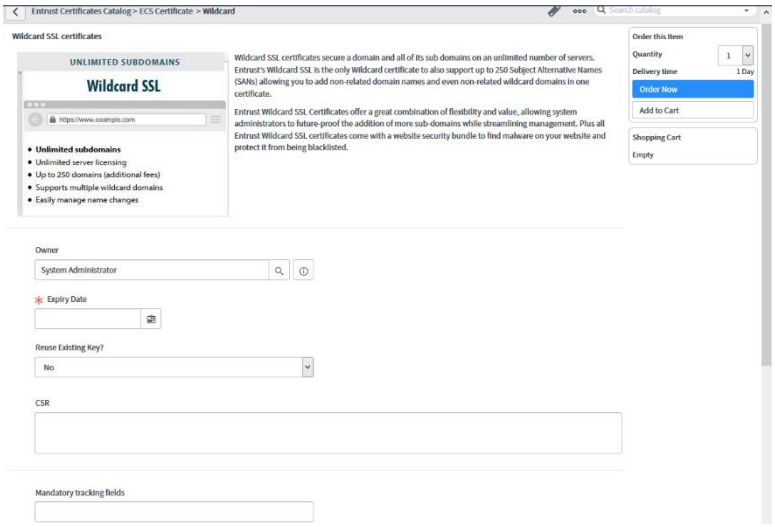
Note: When renewing a certificate, the domain in the common name of the DN (for example, cn=1234.example.com) cannot be changed. A CSR (Certificate Signing Request) containing a different cn from the original certificate, will be rejected by the renewal form.

To renew a certificate

1. Navigate to the **My Certificates** page.
2. Locate the certificate in the grid and right-click the entry to open the context menu.
3. In the context menu, select **Renew** (not currently available for certificates generated from the CA Gateway).



The order certificate page for the type of certificate you are renewing (for example, Wildcard certificate) opens with the **Organization**, **Organizational Unit**, **SAN**, and **Extended Key Usage** fields prefilled.



4. Specify the new expiry date.
5. If you select **Yes** in **Reuse existing key** you do not need to enter a CSR. However, consider creating a new CSR. Creating new keys when you renew a certificate is considered more secure.
6. If the certificate type permits, you can add additional domains to the **Subject Alternative Name**. Adding domains may consume more SAN licenses from your Entrust Certificate Services account. For information about a certificate type (Extended Validation, for example), expand **preview**. For additional information about certificate types, visit our web site using this link.
7. Any previously entered custom fields will be pre-filled. You must fill in all the fields that are marked as *mandatory for the API* in Certificate Services.
8. When you have finished filling out the form, either add it to the cart or click **Order Now**.

   If you chose to reuse the existing key, confirm your choice.