ENTRUST
SECURING A WORLD IN MOTION.

MANAGING PUBLIC TRUST SSL/TLS CERTIFICATES WITH ENTRUST CONNECT FOR MICROSOFT AZURE

Release: 1.0.0

Document issue: 1.0

Date of issue: December 2021

Help us to improve our documentation. Please click this link. and take our survey.

Table of contents

Revision, audience, and guide information

Revisions

Revision	Section	Description
1.0		First release of guide

Audience

This guide is intended for Entrust Certificate Services (ECS) users who need to manage public trust SSL/TLS certificates using Connect for Microsoft Azure and Microsoft Key Vault.

Viewing this guide

Although this guide can be printed, it relies on hyperlinks to other sections. It is best viewed and used electronically.

Prerequisites

This guide assumes that your company already has:

- an ECS account and certificate inventory
- a connection from Connect for Microsoft Azure to the Entrust Certificate Services account through the REST API
- a Microsoft Azure account
- downloaded the Connect for Microsoft Azure app from the Azure Marketplace
- have a Key Vault set up with the ECS Standard OV SSL certificate and REST API credentials. See Integrating Entrust Certificate Services with Azure Key Vault.

About Entrust Connect for Microsoft Azure

This guide describes how to manage Entrust SSL certificates using the Entrust Certificate Services Azure Marketplace app, **Entrust Connect for Microsoft Azure**.

Connect for Microsoft Azure allows you to request and manage Entrust SSL Certificates in your Azure Key Vault.

System Requirements

Browsers:

- Google Chrome – latest release
- Mozilla Firefox – latest release
- Apple Safari – latest release
- Microsoft Edge – latest release

Managing certificates in Entrust Connect for Microsoft Azure

When you connect the Entrust Certificate Services account to your Azure Key Vault using Connect for Microsoft Azure, you can store and manage your certificates directly within the Key Vault.

The Key Vault is also where the Public/Private keypair is generated, and where newly issued certificates will be installed.

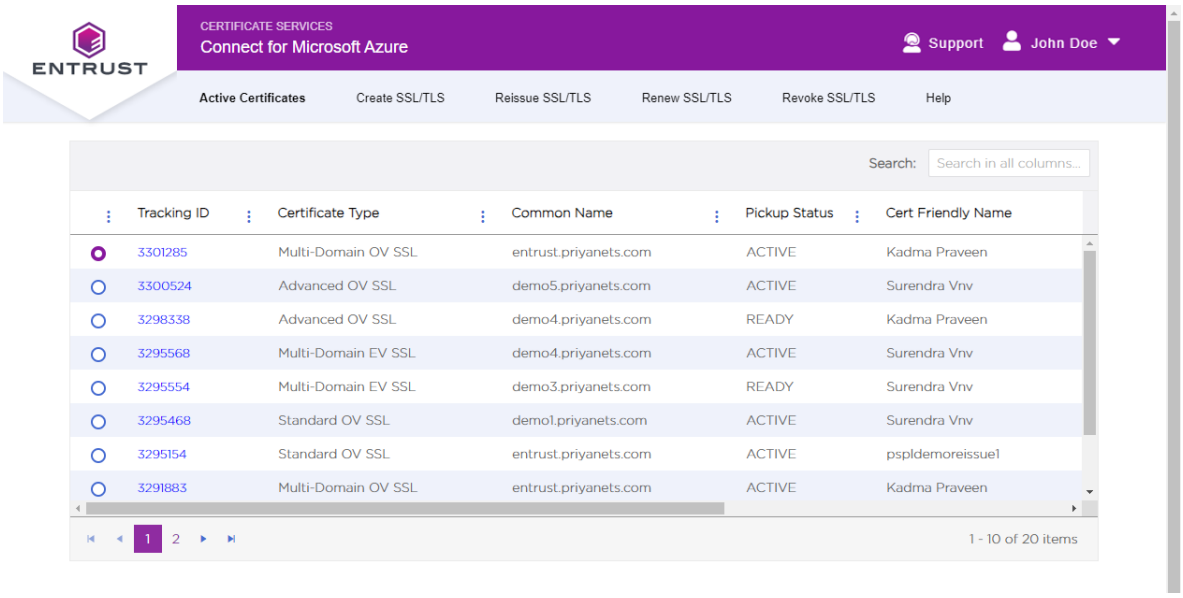
What you can do from the Connect for Microsoft Azure user interface:

- View certificates
- Create a new SSL/TLS certificate
- Install an SSL/TLS certificate
- Reissue an SSL/TLS certificate
- Renew an SSL/TLS certificate
- Revoke an SSL/TLS certificate

View certificates

When you log into Connect for Microsoft Azure, the home screen displays a grid in which all your certificates are listed. This list is retrieved from your ECS account.

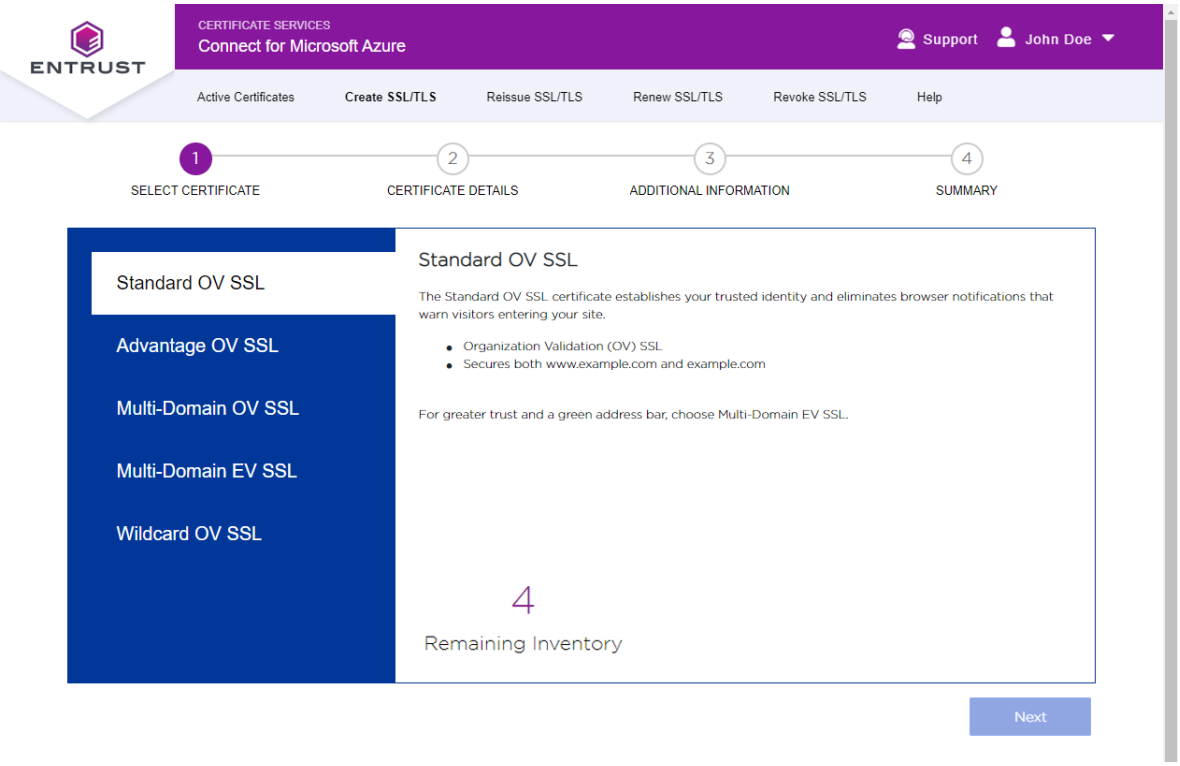
You can create new certificates from this screen, or reissue, renew, or revoke them.



Create a new SSL certificate

You can create Entrust SSL/TLS certificates, both Organization Validation (OV) level and Extended Validation (EV) level, and with different numbers of SANs included:

- Standard OV SSL
- Advantage OV SSL
- Multi-Domain OV SSL
- Multi-Domain EV SSL
- Wildcard OV SSL



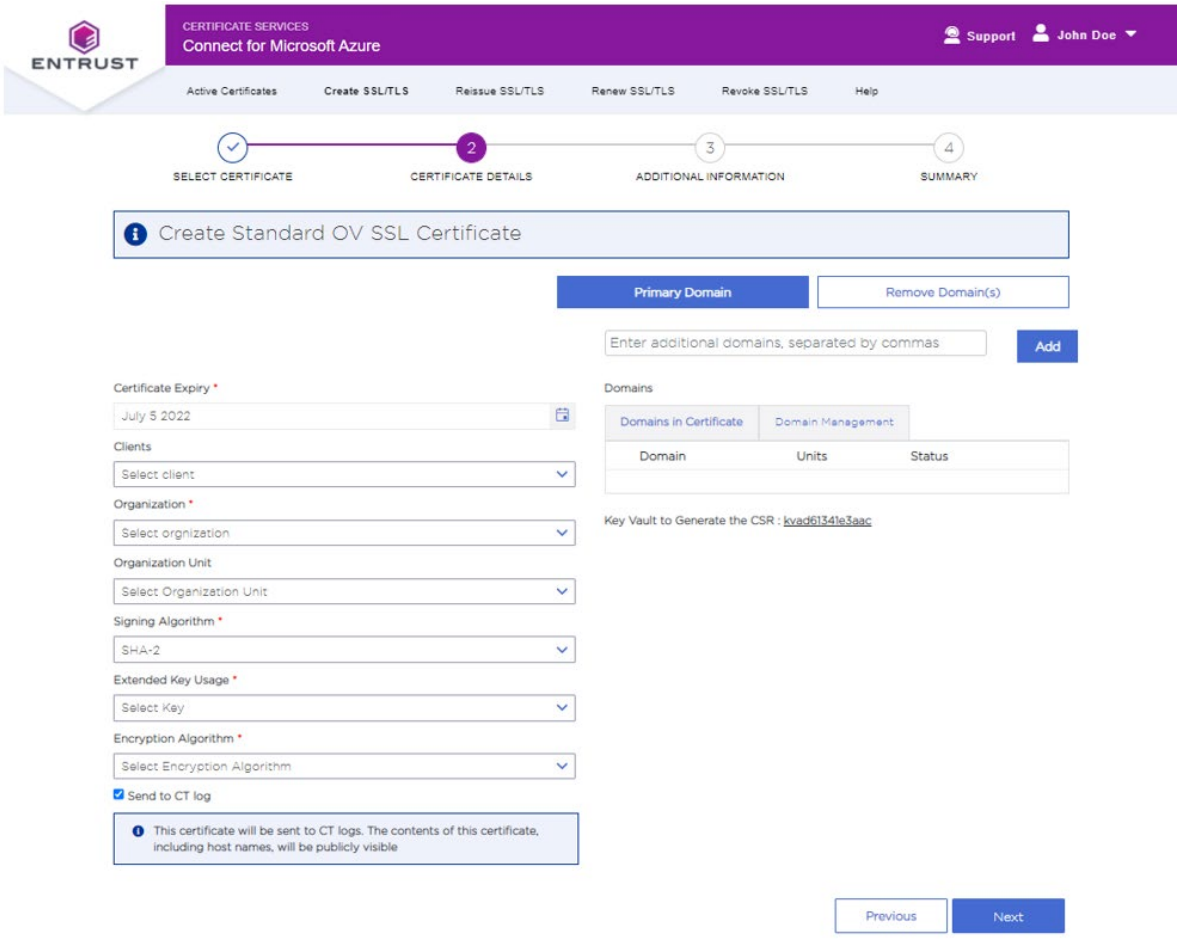
To create a new certificate

1. Click **Create SSL/TLS**.
2. Select the type of certificate you want to create. Each certificate page lists the features of the certificate type.

   NOTE: If Remaining Inventory is displayed as 0 (zero), you will not be able to proceed. Please contact your Certificate Administrator to add inventory for you.

3. Click **Next**. The **Certificate Details** page appears.
4. In **Certificate Expiry** field, select or enter the date the certificate will stop being valid. The maximum lifetime is predefined, which will limit the date selection.

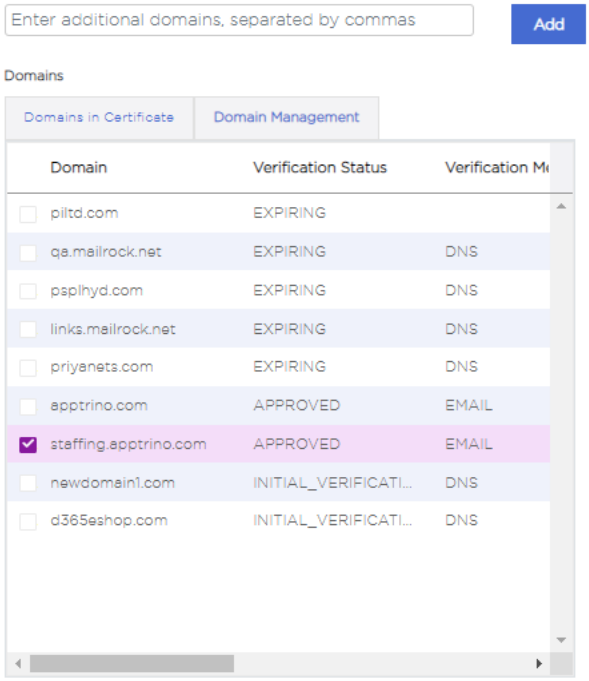
5. In the **Clients** field, select one of the predefined clients. The Client you select will determine the list of Organizations you have access to.
6. In the **Organization** field, select one of the organizations. These organizations have been pre-approved as part of the Client.
7. Optional: Select an **Organization Unit**.
8. In **Signing Algorithm**, select **SHA-2**. This is currently the only option available.
9. In **Extended Key Usage**, select the option that corresponds to the planned use for the certificate. If you are unsure, select **Server and Client Authentication**.
10. In **Encryption Algorithm**, select RSA or ECC. ECC is not available for the Standard OV SSL certificate.



11. In domains, enter one or more domains, or select the domains to use from the **Domain Management** tab. After entering or selecting each domain, click **Add**.
The first domain will be the **Primary Domain**, by default. The Primary Domain will appear in the certificate as the Subject CN. Additional domains will appear as Subject Alternative Names (SANs).

To see the domains you have added to the certificate, click the **Domains in Certificate** tab.

NOTE: The domain(s) you add to the certificate must be verified and available for use (not expired).



12. To change the Primary Domain, click the **Domains in Certificate** tab, select the domain you want to use in the certificate, and click **Primary Domain**.

    NOTE: Below the Domains section of the screen, you will see the name of the Key Vault being used. This is where the Public/Private keypair is generated, and where the new certificate will be installed.

13. Click **Next**. The **Additional Information** page appears.
14. The fields on the Additional Information page are defined in the Certificate Services Enterprise account by your Certificate Administrator. At a minimum, you must complete the fields that are shown as mandatory (red * beside the field name).
15. Click **Next**. The **Summary** page appears.
16. Check the list of selections to ensure accuracy. If any fields need to be changed, click Previous to return to the field and change the field entry.
17. When the **Summary** shows the values you require for the certificate, click **Submit** to generate the certificate.

Reissue an SSL/TLS certificate

If an existing certificate needs to be changed, for example, you can reissue it. Following best security practice, reissuing a certificate results in generating a new Public/Private key pair in Key Vault.

To reissue an SSL certificate

1. On the **Active Certificates** view, select a certificate on the grid.
2. Click **Reissue SSL/TLS**.
3. Follow the instructions in To create a new certificate, starting from Step 3.
4. When you reissue a certificate, the original certificate is revoked. The Reissue process allows you to decide whether to revoke the original certificate immediately, or to schedule the revocation for 30 days in the future. This is a useful option in the case where you need time to make sure the original certificate can be removed without affecting operations on your site.

Renew an SSL/TLS certificate

For a certificate that is approaching expiry, you can renew it. In best security practice, renewing a certificate results in generating a new Public/Private key pair in Key Vault.

To renew an SSL certificate

1. On the **Active Certificates** view, select a certificate on the grid.
2. Click **Renew SSL/TLS**.
3. Follow the instructions in To create a new certificate, starting from Step 3.

Revoke an SSL/TLS certificate

If an existing certificate has been compromised, or is no longer needed, you can revoke it.

NOTE: This action cannot be undone.

To revoke an SSL certificate

1. On the **Active Certificates** view, select a certificate on the grid.
2. Click **Revoke SSL/TLS**.
3. On the screen that appears, check the certificate details to ensure that you are revoking the right certificate.
4. In **Reason for Revocation**, select the reason for the revocation.
5. In **Revocation Comments**, enter the detailed reason. This field is mandatory.
6. Click **Confirm**.

Troubleshooting

This section lists problems or error messages you might encounter during or after the Azure integration, along with advice for their resolution.

"The API client certificate has expired. Please replace or update your Entrust Certificate Services configuration and add an active TLS/SSL certificate."

Cause of the problem:

You will see this error message if the TLS/SSL client certificate that is bound to the ECS REST API expires. Note that the certificate is valid for a period of 12 months.

How to fix the problem:

1. Log in to Certificate Services Enterprise.
2. Navigate to **Administration** > **Advanced Settings** > **API**.
3. Click the pencil icon in the row for the API credential you need to update.
4. Click **Select a Certificate** and click a new certificate from the list. Note the **Tracking ID**.
5. To find and download the new certificate, navigate to **Certificates** > **Managed Certificates**.
6. Search for the certificate Tracking ID and click the certificate row to open the Certificate Details dialog box.
7. Click **Download** to download the TLS/SSL client certificate.
8. Replace the expired TLS/SSL client certificate within Microsoft Azure Key Vault with the new, valid TLS/SSL client certificate.

"Please check the Entrust Certificate Services account to ensure that the API Username is valid."

Cause of the problem:

You will see this error message if the API username, password, or TLS/SSL client certificate are invalid.

How to fix the problem:

To resolve this issue, please double check that the following parameters are correct:

- API username
- API password
- TLS/SSL client certificate is active and bound to the API. (To solve this problem, see “The API client certificate has expired. Please replace or update your Entrust Certificate Services configuration and add an active TLS/SSL certificate.” above.)

“Please check that the Entrust Certificate Services account is still valid.”

Cause of the problem:

You will see this error message if the Entrust Certificate Services account is expired.

How to fix the problem:

Contact your Entrust Sales Representative to renew or extend the term of your Entrust Certificate Services account.