

ENTRUST

Certificate Services Enterprise Enrollment Guide

Release: 13.2.1

Release Date: February 2022

Document issue: 1.0

Entrust and the Hexagon Logo are trademarks, registered trademarks and/or services marks of Entrust Corporation in the U.S. and/or other countries.

All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

© 2022 Entrust Corporation. All rights reserved.

Enrolling in Entrust Certificate Services Enterprise

This guide contains the following sections:

- [“Enrolling in Entrust Certificate Services Enterprise” on page 4](#)
- [“Logging in to Entrust Certificate Services” on page 9](#)

What is Entrust Certificate Services Enterprise?

Entrust Certificate Services Enterprise accounts allow you to purchase and manage an inventory of different types of certificates, according to your needs.

Enrolling in Entrust Certificate Services Enterprise

Follow the instructions in this document to enroll for an Entrust Certificate Services account. Live Chat is available from this site, if you have questions.

To enroll for an Entrust Certificate Services account

- 1 Open the Purchase Enterprise Account page.
(https://buy.entrust.net/index.html?&_ga=2.45312992.532596256.1510601831-1365650293.1510601831#/enterprise/quoteOrder)
- 2 If your organization headquarters are outside the United States, Canada, or the United Kingdom, select that check box under the **New Account Price**.
- 3 Select the **Account Type** you want to use. If you select **Subscription**, specify a lifetime.

Subscription account

- When you enroll for a Subscription account, you specify the lifetime of the account. The **certificate licenses** that you purchase have the same lifespan as the account. When you create an SSL certificate, it uses one license. The lifespan of the certificate is independent of the license and the account. If the certificate expires before the certificate license, the license becomes available to create or renew another certificate of the same type. You can purchase multiple licenses for any type of SSL/TLS certificate sold by Entrust, one for each certificate required.
- If you enroll for a Subscription account, only your SSL/TLS certificates will follow the Subscription model. Other types of Entrust certificates follow the Unit-based model, even if you are using a Subscription account.

Example 1:

- You specify a 2 year account and you purchase an Advantage OV SSL certificate license. The license automatically has a 2 year lifespan.
- You create a 1 year Advantage OV certificate using the license.
- When the certificate expires, that Advantage OV certificate license is still valid and becomes available for use. The license can be used to renew the certificate or to create another Advantage OV certificate.

Example 2:

- You enroll for a one year account and purchase an Advantage OV SSL license. The license has a 1 year lifespan.
- You create an Advantage OV certificate with a 2 year lifespan.
- The Advantage OV license will be in use for the full year of the account lifetime.

- The account and its corresponding licenses expire after one year and for the certificate to remain valid, you need to renew the license (since you paid for one year).
- If you choose not to renew, the certificate will be revoked by Entrust. Entrust issues reminders about expiry ahead of time.

Unit-based account

- If you enroll for a Unit-based account, your account has no inherent lifespan. To create certificate inventory for your account, you purchase **certificate lifetime units**. Each unit represents one year of life for that particular type of certificate.
 - For example, if you purchase 3 Advantage OV SSL units, you could create 3 certificates, each with a one year lifespan or 1 certificate with a two year lifespan and 1 certificate with a one year lifespan, and so on.



Note:

The maximum lifetime for new SSL certificates is 13 months. This maximum applies to all SSL certificates: Standard OV, Advantage OV, Multi-domain OV, Multi-domain EV, Private SSL, and Wildcard OV SSL certificates.

- 4** In the **Product Selection** pane, purchase your initial certificate license or certificate unit inventory. You are not purchasing certificates. These are the licenses or units (depending on the model chosen) that you will use to create certificates through your Certificate Services account.

Your minimum initial inventory must include either:

- 5 SMIME Enterprise certificate units
OR
 - 10 Mobile device certificate units
OR
 - one certificate license or unit of any other type
- a** Select the product (**Advantage OV SSL**, for example).
 - b** Specify the number of licenses or units (the price appears beside the quantity).
 - c** Click **Add to Cart**.
 - d** Repeat for the type and amount of inventory required.

**Note:**

You can add more inventory or exchange the type of inventory purchased at any time using your Certificate Services account.

- 5** In the **Organization Names** pane, add the names of the organizations for which you maintain domains. Entrust will verify that you have the right to maintain domains for these organizations and that they have the right to use the domains.

Be sure to enter the legal name of the organization precisely as it is specified in its papers of incorporation, registration, or accepted equivalent, including punctuation and letter case. Errors in this information will result in delays.

You can enter a maximum of 10 organization names during enrollment. Additional organizations can be added later through Certificate Services.

- 6** In the **Domain Names** pane, add the names of the domains where you will install certificates. Entrust will verify that you have the right to these domains, either because you own the domain or because you maintain the domain for a client who owns the domain. You must enter each domain name correctly to prevent validation problems.

You can enter a maximum of 10 domain names during enrollment. Additional domains can be added later through Certificate Services.

- a** Either:

Enter each name individually in the **Domain Name** field and click **Add**.

OR

Click **Add Multiple Domains** and enter a comma-separated list of domains in the popup dialog box.

**Note:**

Domain validation expires. Entrust can validate domains again to maintain their valid status. Certificate Services provides an interface that enables your administrator to track the status of your domains and submit them for validation.

- 7** Domains verification is done in an automated way. Select the **DNS Verification Method**, or select **Contact Me (Manual)** if you need will need help setting up DNS verification.
- 8** Click **NEXT**.
- 9** On the **Contact Information** page:
 - a** Enter the requested information for each contact.

You can have more than one Account Administrator contact (select **Add Another**). Having more than one contact increases the probability that an Account Administrator will be reachable.

- b** Click **Next Contact** or use the down arrow in the title bar for any contact type to open that information page.

If the same person will act as more than one contact type, you can transfer information from one form to the next using the **Copy contact from** menu.

- c** Click **NEXT**.

To avoid delays, the Higher Authority and Contract Signer contacts must be available to reply when contacted by Entrust. These contacts appear if Extended Validation (EV) certificate licenses or units are included in the initial account request. The Higher Authority contact should be a senior person in the company with the authority to authorize the purchase.

10 On the **Payment** page:

- a** Enter the requested information for the person to whom the credit card is issued. You can use the **Copy contact from** menu, if applicable.
- b** Enter the credit card number and CVV (Card Verification Value).
- c** Read the agreement and click **I have read, understood and accept** to continue.
- d** Click **Buy Now**. Confirmation that your order has been sent to Entrust appears. You can use the link provided to track the progress of your order.

What happens next?

Entrust verifies the following information before creating your account for the Organization Validation (OV) level. Validation of your subscription will be more detailed if EV licenses or units are included.

- Your company has the legal right to conduct business under the name you provided in your order.
- Your company is the registered owner of the domain names provided in your order, or your company has permission to manage the domain or domains.
- The company name in the subscription matches your legally registered name, trade name, or that of a majority-owned subsidiary.
- The contacts provided are employed by your company and have the right to act for your company.

If the information provided in your application is correct and complete, the verification process typically takes three to five business days. If there are problems verifying the information you provided, an Entrust Verification Specialist will contact you.

When your subscription has been verified, Entrust will send you an email message with instructions for logging in to your new Certificate Services account.

Logging in to Entrust Certificate Services

The first time you log in to Entrust Certificate Services, you will use your user name and password—your first factor authentication. After you log in, you will be prompted to set up second factor authentication for your account. You can choose one of these second-factor authentication methods:

- soft token
- Entrust IdentityGuard grid or eGrid
- one-time password (OTP) via SMS message or email

Question-and-Answer (Q&A) authentication is available as a method of accessing the Entrust IdentityGuard Self-Service application if you have forgotten your password.



Note:

If you have trouble setting up your second-factor authentication, see the online help (**Help > Online Help**).

Log in to Entrust Certificate Services: <https://cloud.entrust.net>.

For Certificate Services support by email: ECS.Support@entrust.com.

Figure 1: First factor authentication—user name and password

Certificate Services Login 日本語

Username:
1308060140

Password:
[Masked]

Remember my username

Log In

[Forgot your username?](#)
[Forgot your password?](#)

Have Login Questions? [Login FAQ](#)

Topics in this section include:

- [“What are soft tokens?” on page 10](#)
- [“What are grids/eGrids?” on page 12](#)
- [“Using a one-time password \(OTP\) for second factor authentication” on page 13](#)

What are soft tokens?

Entrust offers a utility for your computer or mobile device that acts like a hardware token. After it is installed and configured, the utility generates a single-use number (security code) that expires after 30 seconds. The utility can create multiple identities for authentication to different applications.

If you decide to use soft tokens for Entrust Certificate Services authentication, the second factor challenge asks you for the number generated by the Entrust IdentityGuard Soft Token utility.

The Entrust IdentityGuard Soft Token utility is offered for download at no cost from Entrust Certificate Services Web site when you configure your account. Installation and registration of the soft token utility is simple and takes just a few moments.

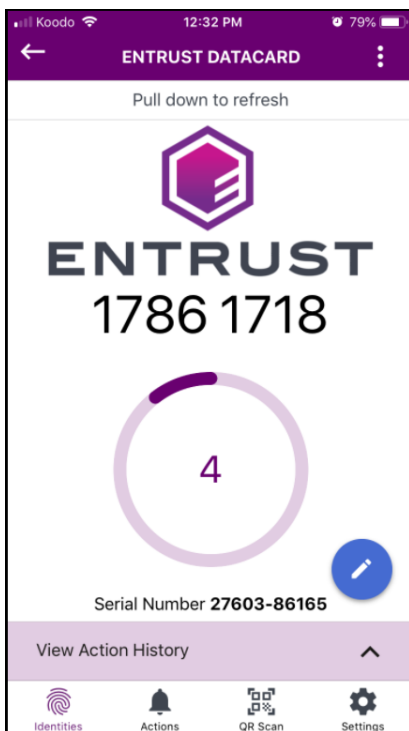
Additional information about Entrust IdentityGuard Soft Token application is available from the utility help—click the Information icon.

Figure 2: Entrust Certificate Services soft token challenge

* Enter a response using the token with serial number 79965-61614:

Open the soft token utility, and enter your PIN. Type the displayed security code into the Challenge field in the log in page and click **OK**. The remaining lifetime of the code is indicated by the **Lifetime** bar below the code.

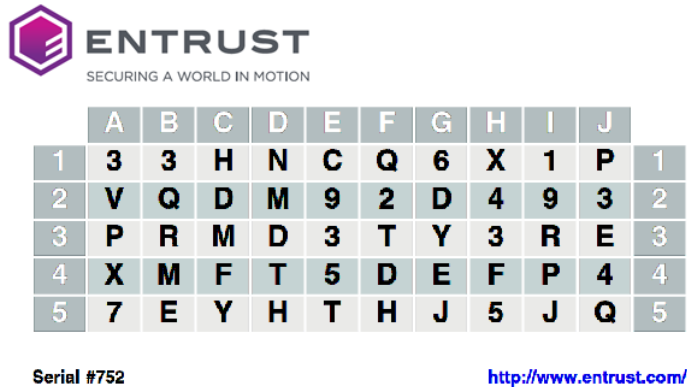
Figure 3: Application displaying code



What are grids/eGrids?

A physical grid card is a grid printed on a card and mailed to you by Entrust. An eGrid is a password-secured PDF graphic of an Entrust IdentityGuard grid that you can download when you set up your account, as shown in the figure.

Figure 4: Entrust grid



When you log in to your account you are asked to enter characters from randomly selected positions in your grid.

In this example, you would answer the Challenge by entering T 4 P.

Figure 5: Grid challenge

Please respond to the following challenge using the grid with serial number 5224:

[C3] [C5] [J3]

.	.	.
---	---	---

OK

[I have misplaced my Grid card](#)

Use the use the letter (column) and number (row) combinations to locate the characters requested in the challenge and enter them in the space below.

Grids in PDF format (eGrids) are available for download from the Entrust Certificate Services site when you configure your Entrust Certificate Services account.

Using a one-time password (OTP) for second factor authentication

If you decide to use an OTP for second factor authentication, provide a mobile phone number or email address to receive the authentication code. When you are prompted for second factor authentication, you will receive a text message/email containing the OTP. Enter the OTP into the **Challenge** field, and click **OK**. The OTP is time-limited.

