Certificate Services Enterprise Enrollment Guide

Release: 13.7

Date of issue: October 2023

Document issue: 1.1

1

Enrolling in Entrust Certificate Services Enterprise

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

This guide contains the following sections:

- “Enrolling in Entrust Certificate Services Enterprise” on page 4
- “Logging in to Entrust Certificate Services” on page 6

Enrolling in Entrust Certificate Services Enterprise

Follow the instructions in this document to enroll for an Entrust Certificate Services account. If you have questions, Live Chat is available. You are automatically enrolled for an Entrust Certificate Services account when you purchase a certificate.

To purchase a certificate and enroll for an Entrust Certificate Services account

1 Open the Entrust Certificate Services page: https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates/entrust-certificate-services

2 In the Entrust Certificate Services banner click BUY NOW.

3 Find the type of certificate to buy and click Shop.

4 Select the type of certificate and click Buy.

5 In the page for the certificate type:

  a Select the subscription term. Be aware that this is not the lifespan of the certificate, but rather the length of the subscription. The lifespan of the certificate follows the lifespan recommendations of the CA/Browser forum.

  b Select the payment option—annual or one time purchase. If you select the annual option you can renew the subscription on an annual basis. If you select the one-time purchase option, you may elect to renew at a later date.

  c Select the number of certificate license subscriptions to purchase.

  d Use Extra Domains to protect more than one domain with the same certificate. The number of Extra Domains that you can add depends on the type of certificate or certificates chosen. Extra Domains are added to the certificate's Subject Alternative Name extension.

  If you have additional questions about this process a chat is available on the page.

6 Click Add to Cart.

7 Check your purchase and click Pr t

account. A Starter account can be upgraded to an Entrust Cetifaicate Services Enterptise account as your certfaicate needs increase. The purchased certfaicates appear as inventory in the account.

What happens next?

Entrust sends information about how to activate your Entrust Cetifaicate Services account to the contct specfaied in your order.

Logging in to Entrust Certificate Services

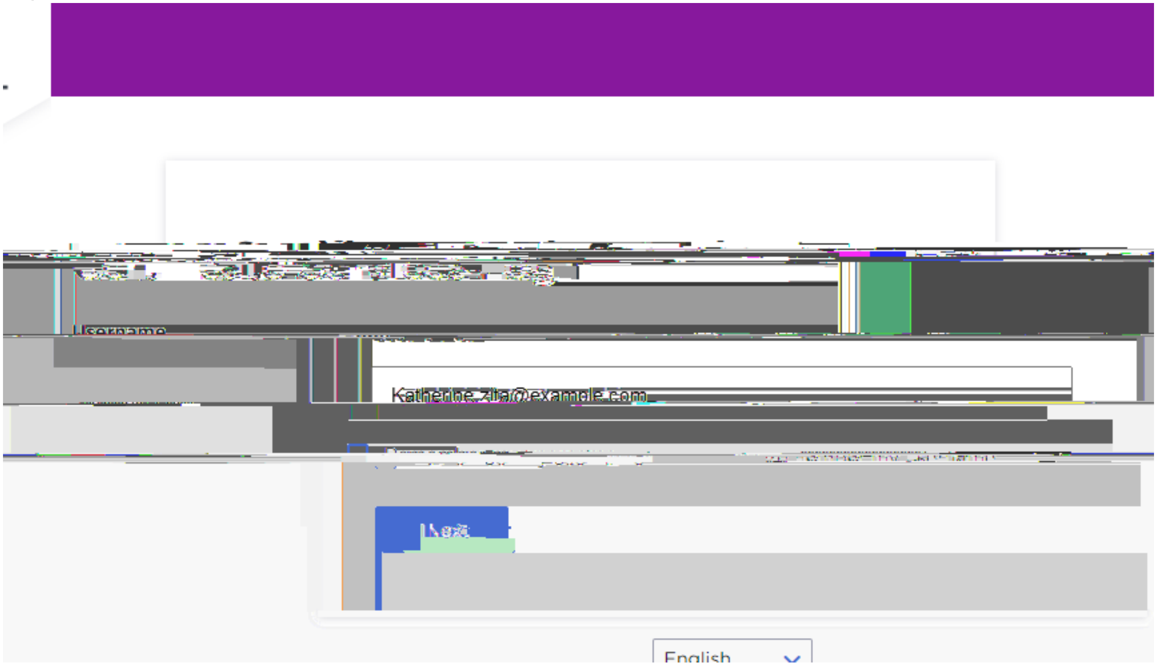
User the link from the email you received to log in to Entrust Certificate Services, you will use your username and password—your first factor authentication. After you log in, you will be prompted to configure:

- the Question-and-Answer (Q&A) authentication feature providing access to your account if you forget your password
- second factor authentication for your account using one of these authentication methods:

  – soft token

  – Entrust IdentityGuard grid card or eGrid

Figure 1: Logon—first factor authentication



Username

Katherine.zita@example.com

Second factor authentication methods

Topics in this section include:

- “What are soft tokens?” on page 7
- “What are grids and eGrids?” on page 8
- “Using a One-time Password (OTP) for second factor authentication” on page 9

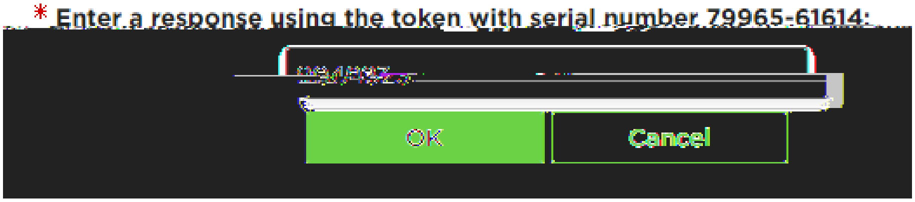
What are soft tokens?

Entrust offers an application for your computer or mobile device that acts like a hardware token. The Entrust Soft Token Identity application is offered for download at no cost from the Entrust Certificate Services Web site when you configure your account options. Consult the help for information about configuring the Identity application. To reach the help, open the app, click the gear icon and scroll to the help entry.

If you decide to use a soft token for Entrust Certificate Services authentication, the Entrust portal login second factor challenge asks you for the number generated by the Identity application.

By default, the Identity application generates a single-use number (security code) that expires after 30 seconds.

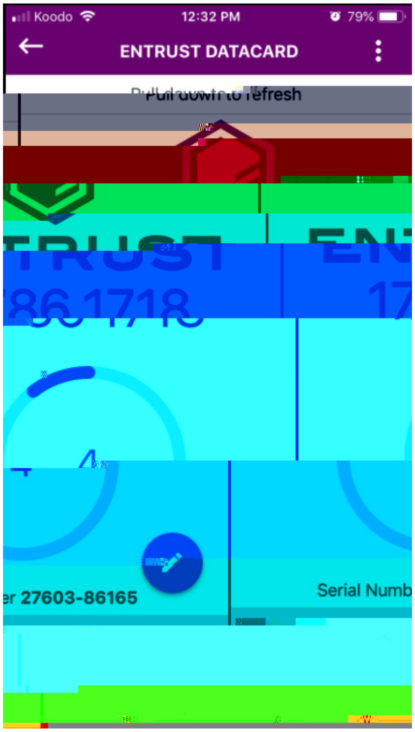
Figure 2: Entrust Certificate Services portal—soft token second factor authentication



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

Open the Identity application, and enter your PIN. Type the displayed security code into the indicated field as shown in Figure 2 and click OK. The remaining lifetime of the code is shown on the indicator below the code as shown in Figure 3. If the remaining lifetime expires before you enter the code, the token generates a different code and the timer resets.

Figure 3: Application displaying code



Koodo 12:32 PM 79%

ENTRUST DATACARD

Pull down to refresh

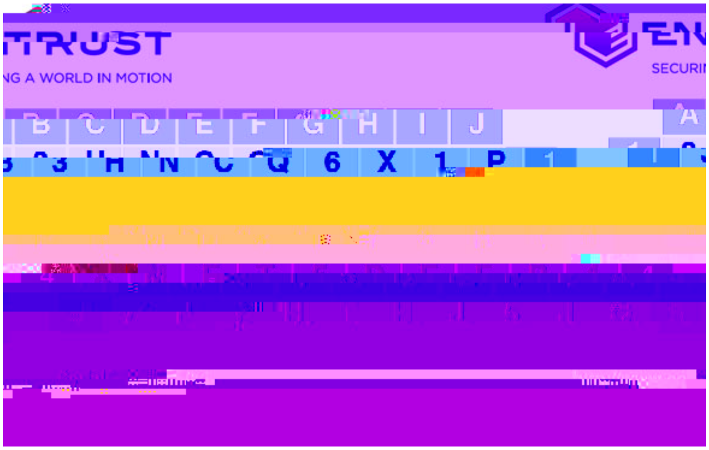
er 27603-86165

Serial Numb

What are grids and eGrids?

A physical grid is printed on a plastic card as shown in Figure 4.

Figure 4: Entrust grid



An eGrid is a password-secured PDF graphic of an Entrust IdentityGuard grid that you can download when you configure your account.

If you select the grid or eGrid second factor option, when you log in to your account you are asked to enter characters from randomly selected positions in your grid. Use the letter (column) and number (row) combinations to locate the characters requested in the challenge and enter them in the space below.

In this example, you would answer the challenge by entering M Y E.

Figure 5: Grid challenge

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, enter the OTP into the OTP field, and click Login