Entrust

Certificate Management Service 10.1

Enrollment Guide

Date of Issue: April 2013

Entrust®
Securing Digital Identities
& Information

Copyright © 2008-2013 Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

Obtaining technical support

For support assistance by telephone call one of the numbers below:

- 1-866-267-9297 in North America
- 1-613-270-2680 outside North America

You can also email Customer Support at:

- ssl@entrust.com

Entrust Certificate Management Service Enrollment Guide

This guide contains information about:

- "Enrolling for the Certificate Management Service" on page 5
- "The verification process" on page 7
- "Logging in to the Entrust Certificate Management Service" on page 8

What is the Certificate Management Service?

If you purchase five or more certificates of the same type from Entrust, you can enroll for the Entrust Certificate Management Service (CMS).

The CMS allows you to purchase and manage an inventory of different types of certificates according to your needs. As your network grows and changes you can use these certificates to establish and maintain secure communication between devices, sign code, secure Adobe Acrobat or LiveCycle documents and forms, or secure email message by signing, encrypting or both.

The Certificate Management Service makes it easy for you to:

- know how many certificates of each type are available for use
- create and assign certificates
- keep track of certificates used by client accounts
- purchase or renew certificates
- add or remove client domains
- add or remove administrator accounts
- delegate certificate request approval
- approve certificate requests

- use Entrust Discovery to obtain detailed information about certificates in your network

Enrolling for the Certificate Management Service

Before you can enroll for the Certificate Management Service (CMS), you must purchase certificates to manage. A minimum purchase of five certificates of one certificate type is required to enroll for a Certificate Management Service account.

Note: You cannot purchase more than 100 certificates online. To purchase more than 100 certificates, contact an Entrust Sales representative.

Purchasing certificates by credit card

To purchase certificates by credit card, you must have a valid Visa®, MasterCard®, or American Express® credit card.

Purchasing certificates by purchase order

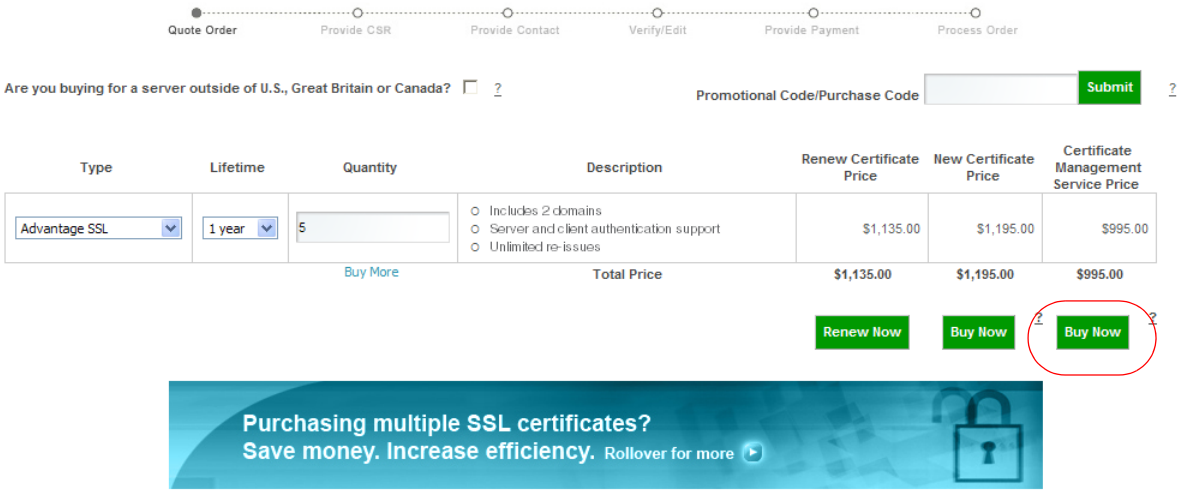
To purchase certificates by purchase order, please contact Entrust Sales at:

- 1-888-690-2424 (toll free within North America)
- 1-613-270-3411 (outside of North America)
- Entrust@Entrust.com

Entrust Sales will provide you with a purchase order code that you can use to purchase certificates online. The enrollment and purchasing process will automatically enter your service lifetime, certificate quantities, organizations, and domain name values the in the online enrollment and purchasing forms.

Note: If your order totals less than $1000.00 you cannot pay by purchase order. Use a credit card to pay for orders totaling less than $1000.00.

To enroll for the Certificate Management Service, simply purchase five or more certificates of a single type. To start the enrollment process, click Buy Now under the Certificate Management Service Price column.



Continue through the wizard and complete the purchase. If you need detailed information about purchasing certificates, separate guides.are available for each type of certificate.

The verification process

Entrust performs a limited verification of the information in your order before creating your account. Entrust verifies whether:

- your organization has the legal right to conduct business under the organization name you provided in your order
- your organization is the registered owner of the domain name you provided in your order
- your organization name matches your legally registered name, trade name, or majority-owned subsidiary.

  Entrust can only issue certificates if your organization name matches the organization name provided in your certificate signing requests.
- the contacts you provided are employed by your organization

If the information you provided in your application is correct and complete, verification process typically takes three to five business days. If Entrust encounters any problems verifying the information your provided, Entrust will contact you immediately.

Contacts

Entrust will contact the people that were listed in the enrollment application. For prompt processing of your request, individuals listed as contacts should be prepared to respond as needed.

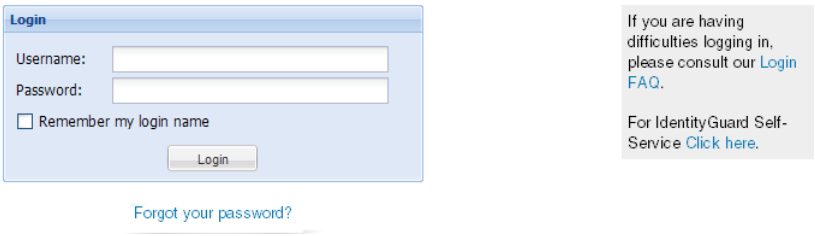
Logging in to the Entrust Certificate Management Service

CMS supports user name and password as primary authentication and second-factor authentication using Entrust IdentityGuard grid, eGrid, or soft token authentication. Question-and-Answer (Q&A) authentication is available as a method of accessing the Entrust IdentityGuard Self-Service application if other authentication methods are unavailable. Second-factor authentication is mandatory for all new users. Existing CMS users without second factor authentication have until June 25, 2012 to register for second factor authentication. Users with existing second factor authentication are unaffected by the change.

Users with the requester role do not require second-factor authentication.

Users can log in to the CMS using the URL https://managed.entrust.net.

Figure 1: Primary authentication—user name and password



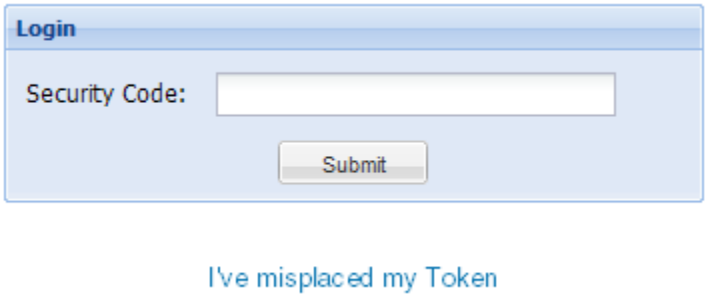
Topics in this section include:

- "What are soft tokens?" on page 8
- "What are grids?" on page 9
- "How to obtain second factor authentication" on page 10
- "Second factor expiry" on page 11
- "Configuring login with second factor authentication—new users" on page 11

What are soft tokens?

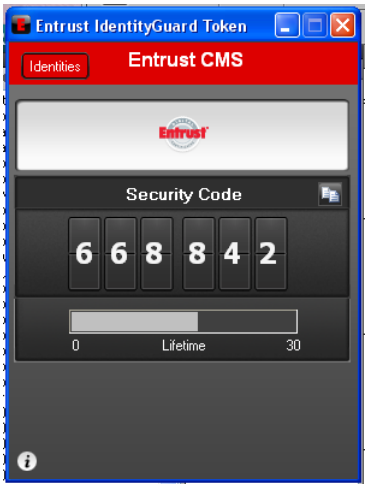
If you decide to use soft tokens for authentication, the CMS challenge asks you for the number created by the Entrust IdentityGuard Soft Token application.

Figure 2: CMS soft token challenge



The soft token application creates a security code. Enter the code into the Security Code field in the log in page and click **Submit**. The code can be used for 30 seconds. After that time a second code is created and displayed and the old code will not work. The remaining lifetime of the code is indicated by the **Lifetime** bar below the code.

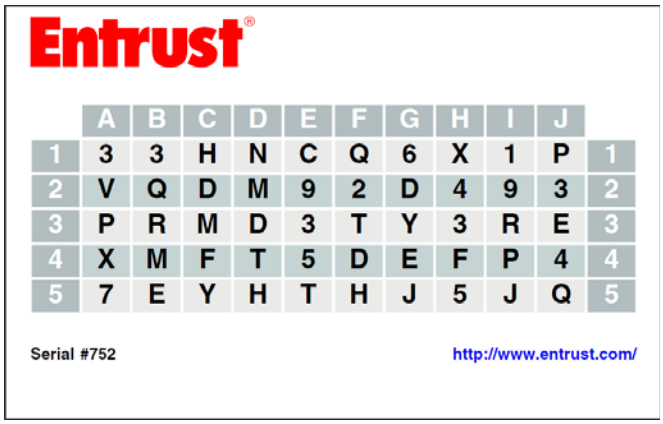
Figure 3: Application displaying code



What are grids?

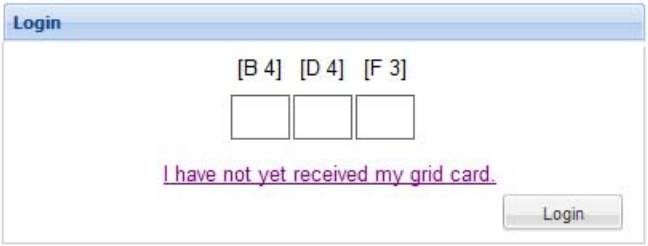
Entrust IdentityGuard eGrids are graphics that display a grid composed of letters and numbers as shown in Figure 4.

Figure 4: Entrust grid



If you are using a physical grid (a grid printed on a card and mailed to you by Entrust) or an eGrid for authentication, when you log in to your account you are asked to enter characters from randomly selected positions in your grid (see Figure 5).

Figure 5: Grid challenge



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.

How to obtain second factor authentication

Administrators choosing soft token for second factor authentication require the Entrust IdentityGuard Soft Token application. The application can be downloaded at no cost from Entrust. Installation and registration of the soft token application is simple and only requires a few moments.

Additional information about Entrust IdentityGuard Soft Token application is available from the application's online help.

Grids in electronic file format (eGrids) or soft token identities can be downloaded from the CMS login pages when an Administrator logs into CMS.

See "Configuring login with second factor authentication—new users" on page 11 for detailed information about configuring second factor authentication.

Second factor expiry

Entrust IdentityGuard grids and eGrids expire 2 years after being issued. Entrust automatically sends a replacement for a physical grid card 60 days before the existing grid card's expiry date. Users who have downloaded an eGrid file can download a replacement when the existing grid expires.

Soft tokens do not expire.

Configuring login with second factor authentication—new users

First-time users receive an email from Entrust confirming the creation of the requested account. CMS sends a second email with a one time password providing access to the CMS. When the new user uses the password to log in to the Web site, they are required to create and change the password and choose and download a form of second factor authentication.

To log in to the Entrust Certificate Management Service as a new user

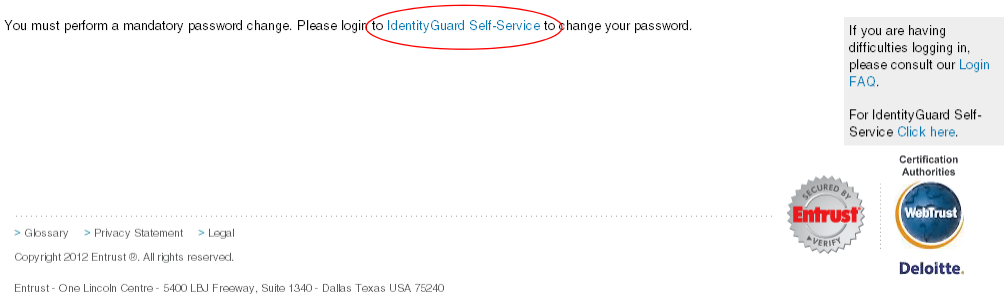
1. New users receive an email from Entrust containing their username and a separate email with your password. Click the link in the email to open the CMS login page in your browser.

   When you log in with your temporary password, if you are setting up the account, the license agreement page appears. This page does not appear if you are adding a user to an existing account. Read through the license agreement and click **Accept** to agree and continue. If you **Decline** this agreement, you cannot log into the CMS.

If you forget your password, use the **Forget your password** link to have a temporary password sent to you. You will be asked to change the temporary password when you log in to CMS.

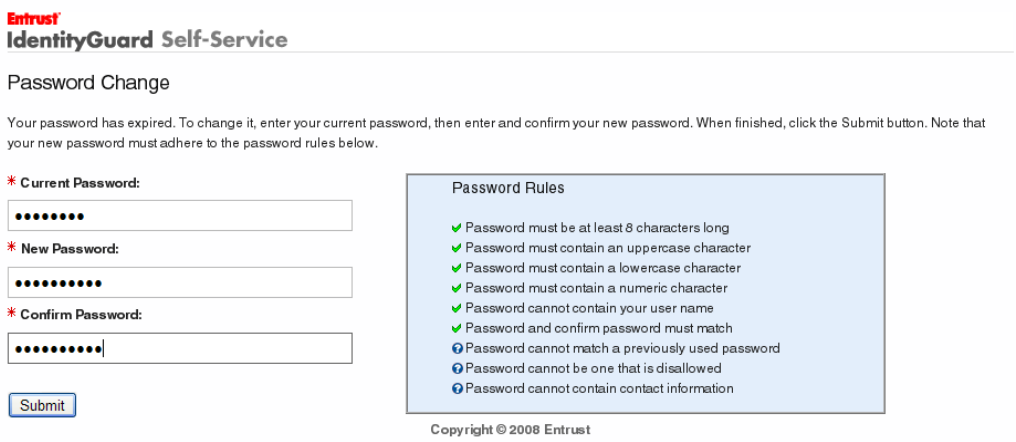
If you log in as a new user, you are redirected to the Entrust IdentityGuard Self-Service Web pages to change your password and obtain second factor authentication.

2 Click IdentityGuard Self-Service.



The **Password Change** page appears.

3 In the **Password Change** page, type the one-time password that was sent to you by Entrust into the **Current Password** field. Enter a new password that conforms to the **Password Rules** into the **Password** field, and again into the **Confirm Password** field.



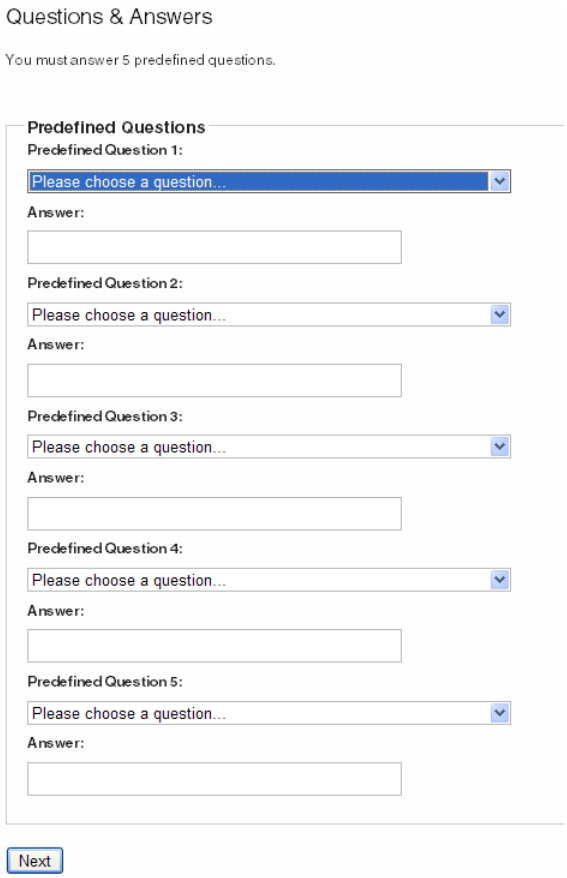
4 Click **Submit**.

Passwords expire after one year. After your password expires, you must create a new password the next time you log in.

---

5 Select questions from the drop-down list and type your answers into the **Answer** field below. These questions and answers can be used later as a means of

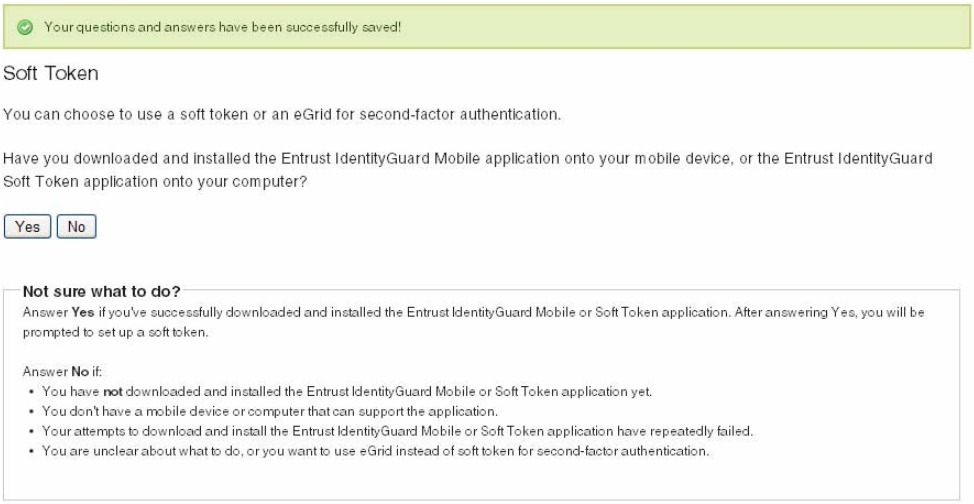
accessing, Entrust IdentityGuard Self-Service if a user cannot use their soft token or grid for some reason.



Select questions and answers that are easy to remember.

6 Click **Next.**

7 CMS offers soft token or eGrid options for second factor authentication. If you decide to use soft token you must download the Entrust IdentityGuard Soft Token application.



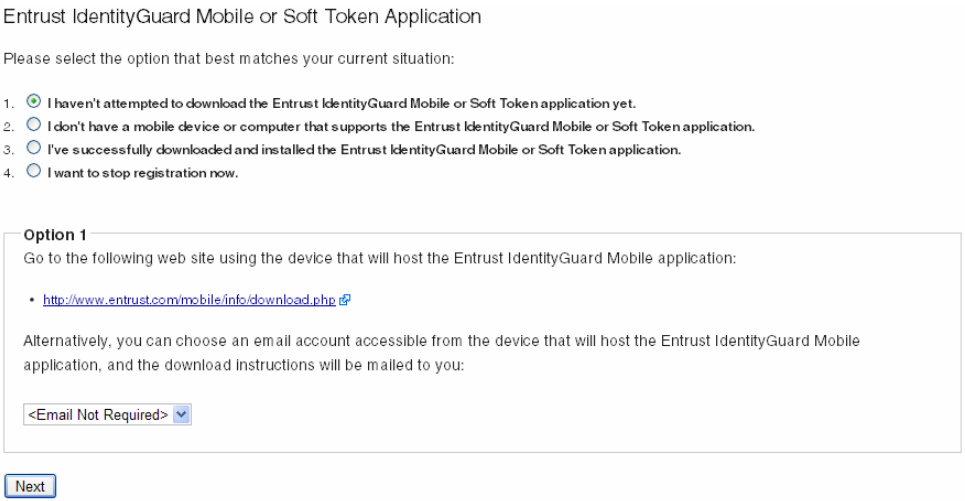
Click **Yes** if you already have the application installed and you want to down load and use a soft token for second factor authentication. If you selected **Yes** go to Step 8 i.

Click **No** if you still need to download the application or you want to use the eGrid option.

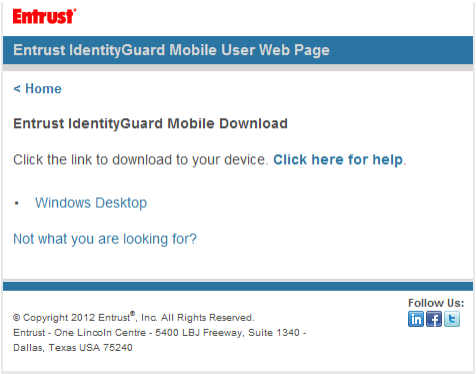
8 If you selected **No** and you want to use a soft token:

a Select the link in the **Option 1** pane, if you are downloading the soft token application to your Windows computer. If you want to send instructions for downloading the soft token application to your mobile device (cellular phone, for example) and your device has access to the email account used by CMS to contact you, select **email** from the drop-down list. By selecting

the link from an email message that is displayed on your mobile device, the web page detects that device and displays a link to compatible software

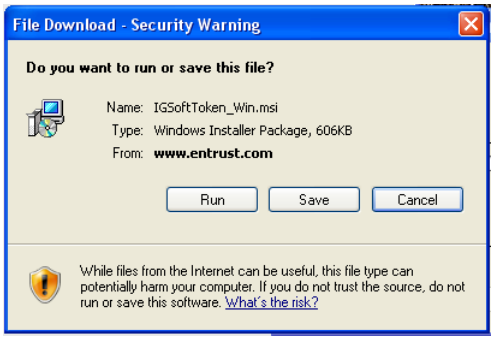


b The download site detects the type of device you are using and presents you with the option of downloading compatible software. If you are downloading the software for a different device, or the option is not correct, use the **Not what you're looking for** link to select the correct download.



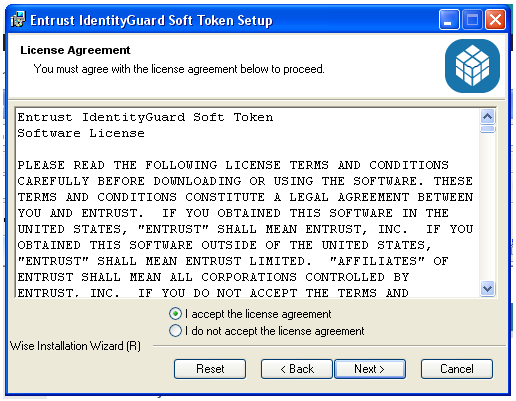
The following graphics and instructions use depict a Windows download and installation. Yours may vary somewhat.

c Run the installation program or save and double-click the executable to run the installer.

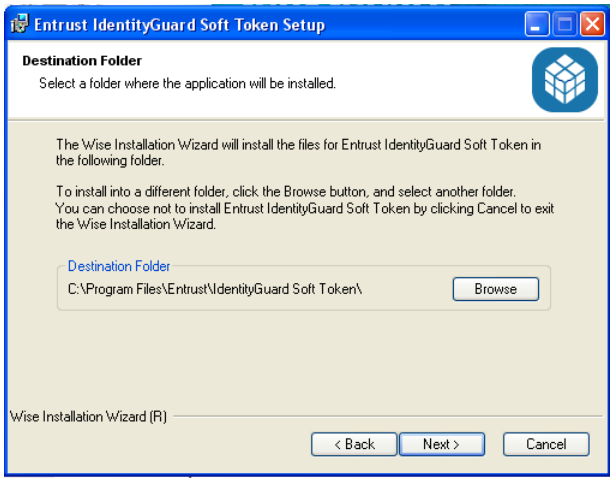


d Click **Next**.

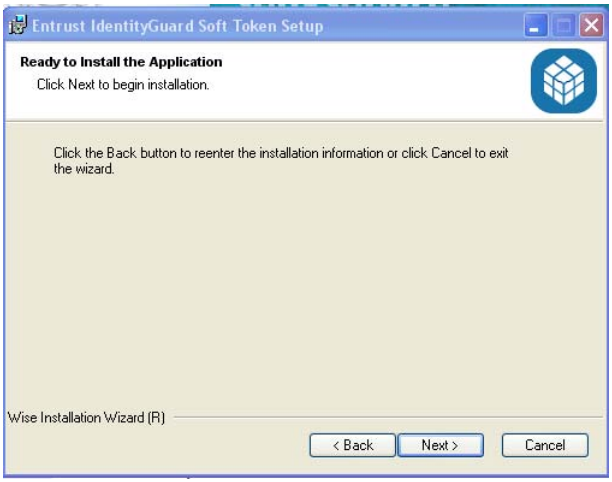
e Accept the license agreement to continue and click **Next**.



f Browse to the location where you want the software installed or accept the default location, and click **Next**.

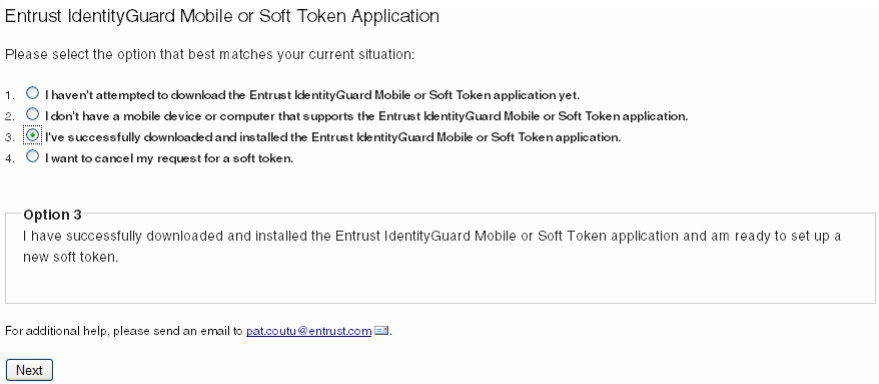


g Click **Next**.



h Click **Finish** to complete the installation.

- In the Entrust IdentityGuard Self Service application, select **I've successfully downloaded and installed**....



- Open the Entrust IdentityGuard Soft Token application. On a Windows desktop this can be found in the **Start** > **All Programs** > **Entrust IdentityGuard Soft Token**

k Copy the highlighted information from the Self Service application page to the soft token as shown in Figure 6. Click **Next** when you are finished.

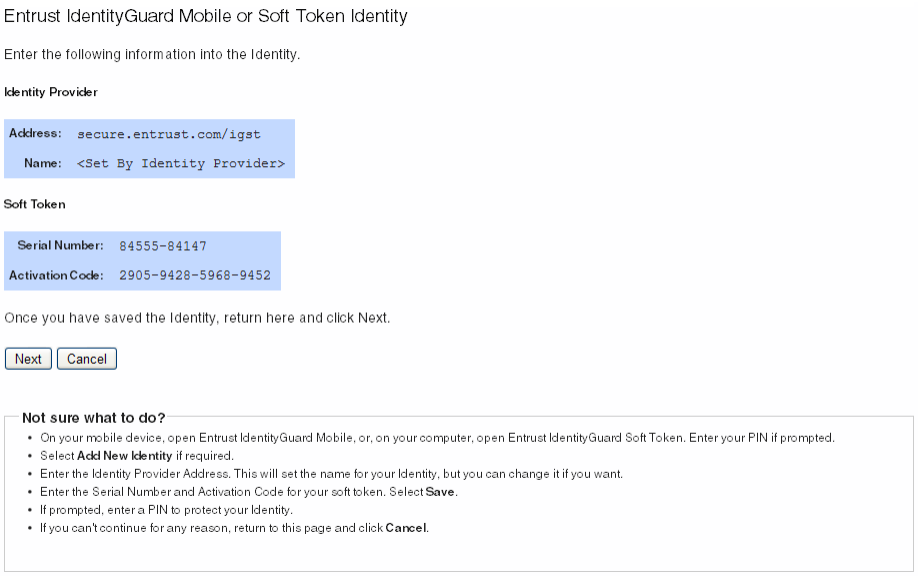
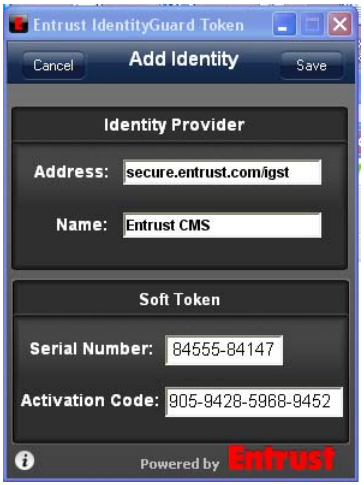


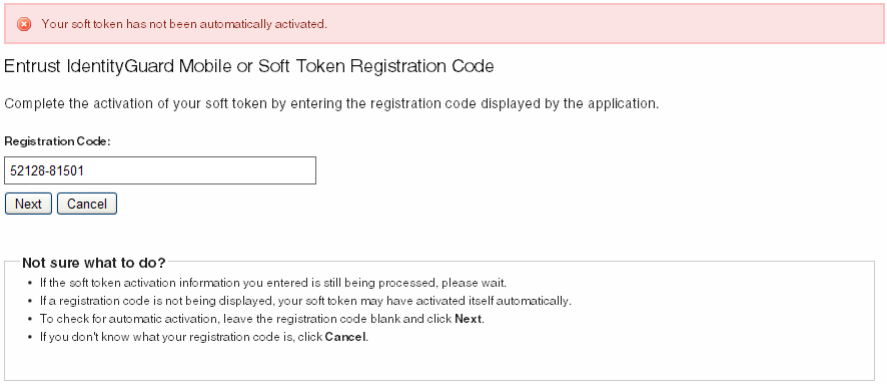
Figure 6: Configuring soft token



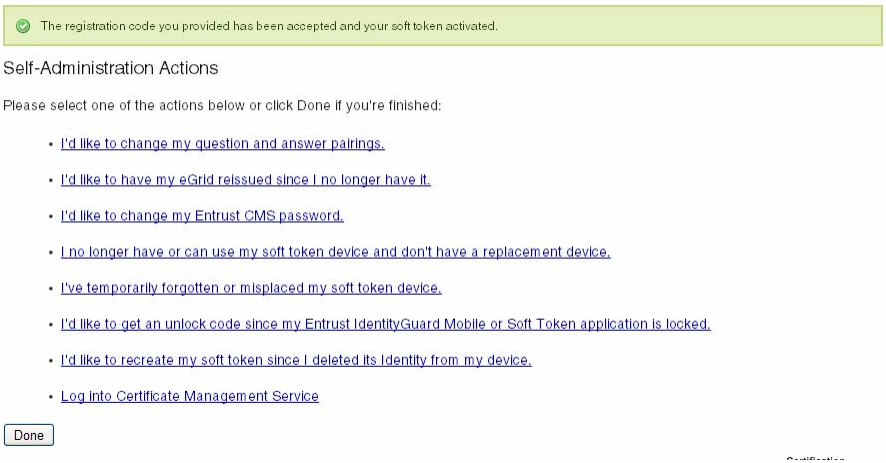
- Set the PIN that you want to use to protect access to the software soft token. Re-enter it to confirm the PIN when asked.

The soft token application displays the registration number.

m Copy the registration number from the soft token to the IdentityGuard Self Service page. Click **Next**.



n The IdentityGuard Self Service application displays other self service options. The soft token is ready for use.



9 If you selected **No** and you intend to use an eGrid for authentication:

a Select option 2 (**I don't have a mobile device or computer that supports**...) Click **Next**.

Entrust IdentityGuard Mobile or Soft Token Application

Please select the option that best matches your current situation:

1. I haven't attempted to download the Entrust IdentityGuard Mobile or Soft Token application yet.
2. I don't have a mobile device or computer that supports the Entrust IdentityGuard Mobile or Soft Token application.
3. I've successfully downloaded and installed the Entrust IdentityGuard Mobile or Soft Token application.
4. I want to stop registration now.

Option 2

Since you have indicated that you are unable to install the Entrust IdentityGuard Mobile or Soft Token application, you will use a grid as a replacement means of providing authentication.

Next

b In the **Please confirm**... page click **Yes**.

Please confirm the following ...

Are you sure that you want to use eGrid instead of soft token for second-factor authentication? If you change your mind you can request a soft token at another time.

Yes No

> Glossary > Privacy Statement > Legal

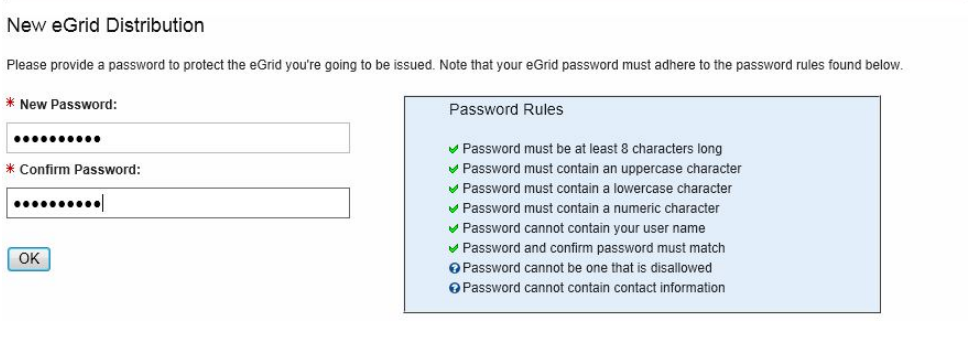
Copyright ©2012 Entrust

Entrust - One Lincoln Centre - 5400 LBJ Freeway, Suite 1340 - Dallas Texas USA 75240

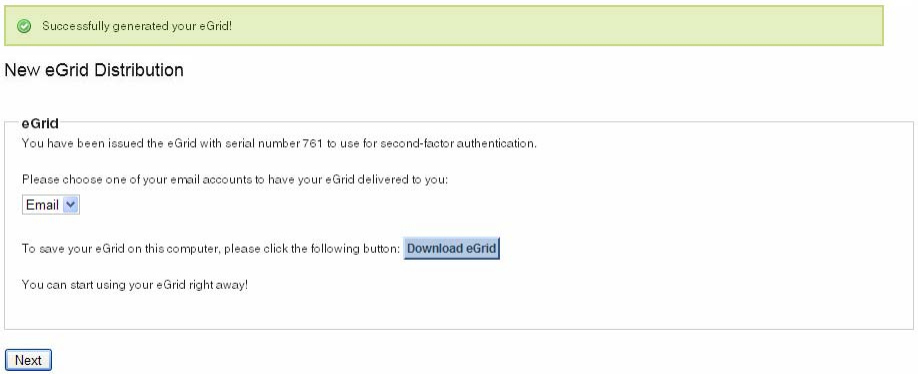
Certification Authorities

c eGrids are password protected. Enter and confirm a password that conforms to the password rules in the Password Rules pane. Each x becomes a check

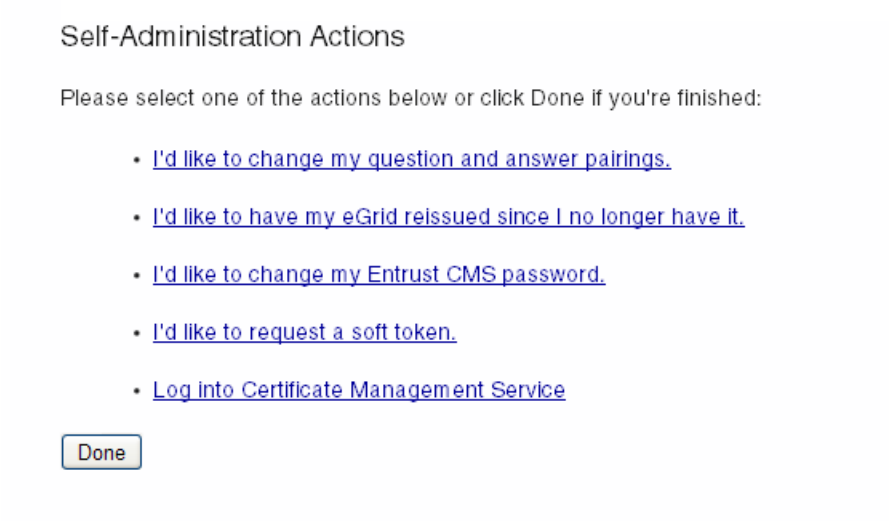
mark if your password conforms to the rule. Click **Next**.when you have finished



d In the Additional Authentication Types page, select **Email** if you prefer to have a link to the eGrid sent to you. This may the useful if you intend to use it from a different device (smart phone, for example) and the device has access to the email account used by CMS. Click Download eGrid to download the eGrid to device you are currently using. The default file name is in the format `<user_ID>-egrid.pdf`



e You are presented with a list of self-service options.



Use your new password and second factor authenticator the next time you log into the Certificate Management Service. To change your password or question and answer pairings, use the **Click here for IdentityGuard Self-Service** link on the **Preferences** >**Account Preferences** or log in page.