Entrust Managed Services PKI™

Getting an end-user Entrust certificate using Entrust Authority™ Administration Services

Document issue: 2.0

Date of issue: June 2009
## Revision information

<table>
<thead>
<tr>
<th>Document issue and date</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue 2.0 June 2009</td>
<td>“Recovering your certificate through Administration Services” on page 7</td>
<td>Added instructions detailing how to recover a certificate.</td>
</tr>
<tr>
<td>Issue 2.0 June 2009</td>
<td>Entire guide</td>
<td>Various copy edits.</td>
</tr>
</tbody>
</table>

---

### Obtaining technical support

For support assistance by telephone call one of the numbers below:
- 1-877-754-7878 in North America
- 1-613-270-3700 outside North America

You can also email Customer Support at:
- support@entrust.com

---

**Copyright © 2009 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.
Entrust certificates for end-users

If you do not have Entrust Entelligence™ Security Provider installed on your computer (Start > All Programs > Entrust Entelligence), you can obtain your digital certificate using a Web-based application, called Entrust Authority™ Administration Services. This application installs your certificate within the Windows framework. Depending on your organization’s requirements, you can also store your certificate on your computer or on a smart card or token.

**Note:** If you do have Security Provider installed, see *Getting an end-user Entrust certificate using Entrust Entelligence Security Provider* available under the Resources tab at [www.entrust.com/managed_services](http://www.entrust.com/managed_services).

At some point, you may be required to recover your user account for various reasons, such as a lost or damaged certificate, a compromised password, or as the result of a change to your certificate. Your administrator generally indicates when you need to perform a recovery. You use the same Web-based application to perform this function as you do to create your certificate.

This guide includes the following topics:

- “Getting your certificate through Administration Services” on page 4
- “Recovering your certificate through Administration Services” on page 7
- “Using your certificate” on page 12
Getting your certificate through Administration Services

To obtain your Entrust digital certificate, you must:

1. Get your reference number and authentication code from your administrator.
   
   The reference number and authorization code, collectively known as activation codes, are needed for enrollment. If you have not received your activation codes, contact your administrator.

2. Access the Web-based application at the URL provided by your administrator and use your activation codes to get your certificate.
   
   Administration Services allows you to create and manage your Entrust certificates. Your administrator will provide you with the URL.

Complete the following procedure to obtain your certificate.

To obtain your certificate through the Web-based application

1. In a browser, enter the URL of the Web-based application.

   **Note:** Contact your administrator if you have not received the URL.

The Entrust User Registration and Self-Administration site appears. The landing page may look different than the screen capture below based on the enrollment model of your organization.

![Entrust User Registration and Self-Administration](Image)
2 Click Create My Digital ID.

The Create Entrust Digital ID page appears.

3 Click Create Third-Party Security Store. This option stores your certificate within the Windows framework.

The Create third-party security store page appears.

4 On the Create third-party security store page, complete the following:
   a Enter the reference number and authorization code in the applicable fields.
Note: If you do not have your reference number and authorization code, contact your administrator.

b Select **Store Entrust digital ID on a smart card** if your organization plans to store certificates on hardware security modules (HSM), such as a smart card or token. Ensure your HSM is connected to your computer.

c Click **Create Security Store**.

5 If you selected to store your certificate on an HSM, enter your PIN.

A security warning dialog box may appear, which says that Windows cannot validate that the certificate is from the certification authority (CA) it claims to be. This is because the root certificate is not in your Windows trusted certificate store.

6 In the Security Warning dialog box, click **Yes** so that Windows stores the root certificate in your Windows trusted certificate store. This also ensures that all certificates your organization’s CA issues are automatically trusted as well.
Your digital ID and related certificate is installed in the location specified (such as your computer or HSM).

**Recovering your certificate through Administration Services**

To recover your Entrust digital certificate, you must:

1. Get your reference number and authentication code from your administrator.
   - The reference number and authorization code, collectively known as activation codes, are needed for recovery. If you have not received your activation codes, contact your administrator.

2. Access the Web-based application at the URL provided by your administrator and use your activation codes to recover your certificate.
   - Administration Services is the same application you used to create your certificate.

Complete the following procedure to recover your certificate.

**To recover your certificate**

1. In a browser, enter the URL of the Web-based application.

---

**Note:** Contact your administrator if you have not received the URL.

The Entrust User Registration and Self-Administration site appears. The landing page may look different than the screen capture below based on the enrollment model of your organization.
2 Click **Recover My Digital ID**.

The **Recover Entrust Digital ID** page appears.
3 Click **Recover Third-Party Security Store**.

The **Recover third-party security store** page appears.
Enter the reference number and authorization code for the recovery in the applicable fields.

**Note:** If you do not have your reference number and authorization code, contact your administrator.

5 Select **Store Entrust digital ID on a smart card** if you are recovering a certificate stored to a token or smart card. Ensure your token or smart card is connected to your computer.

6 Click **Recover Security Store**.

7 If you selected to store your certificate on token or smart card, enter your PIN.
Your digital ID and related certificate is recovered to the location specified (such as your computer or smart card).
Using your certificate

With an Entrust digital certificate, you can:

- sign and encrypt
  - Adobe PDF documents
  - Microsoft Office documents (Excel, Word, Outlook)
  - Windows files and folders
When you add a digital signature to a file or document, you are confirming your identity, ensuring the integrity of the data, and binding your identity to the transaction (non-repudiation).

When you encrypt a file or document, you are ensuring that it cannot be viewed by anyone who does not have the public key that corresponds to the private key that encrypted the file or document.

- authenticate
  - Devices (VPN, handhelds, etc.)
  - Applications
  - Servers
  - Buildings

If you do not know how your organization intends to use certificates, contact your administrator.

The following table briefly describes various ways to use your Entrust certificate and identifies the task-specific guides you can reference for more information.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>See this guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sign and/or encrypt PDF documents</td>
<td>Using Entrust certificates with Adobe PDF files and forms</td>
<td>This guide documents how to configure Adobe to recognize and trust digital certificates, and how to digitally sign a PDF document.</td>
</tr>
</tbody>
</table>

Note: All Managed Services PKI documentation is available under the Resources tab at www.entrust.com/managed_services.
### Table 1: Task and related documentation

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>See this guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sign and/or encrypt Microsoft Office documents</td>
<td>Using Entrust certificates with Microsoft Office and Windows</td>
<td>This guide documents:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Signing and sending messages using Microsoft Word, Excel, and PowerPoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sending secure messages using Microsoft Outlook</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring Microsoft Outlook to use a single certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Removing message encryption in Microsoft Outlook</td>
</tr>
<tr>
<td>sign and/or encrypt files on your Windows operating system.</td>
<td>Using Entrust certificates with Microsoft Office and Windows</td>
<td>This guide documents how to secure Windows files and folders and send a secure message from a Windows folder.</td>
</tr>
<tr>
<td>authenticate to a VPN for secure, remote access to your network</td>
<td>Using Entrust certificates with VPN</td>
<td>This guide includes information about IPsec and SSL VPN, security issues, and VPN authentication mechanisms. It also provides instructions on how to import your certificate into your VPN client and how to configure your router to trust certificates issued to VPN clients.</td>
</tr>
</tbody>
</table>