

Entrust Managed Services PKI Administrator's Quick Start Guide

Each Managed Services PKI organization requires an administrator—also known as a local registration authority (LRA)—whose duty it is to manage end users and their digital IDs. This document describes the processes that the LRA must follow to:

- complete the creation of an administrator digital ID
- set up end users so that they can create their digital IDs

The LRA must complete these processes before end users can begin enrolling for digital IDs. Your end users must install Entrust Entelligence Security Provider for Windows before they can enroll for their digital IDs.

This guide includes the following sections:

- [“Creating an administrator digital ID” on page 2](#)
- [“Log in as an administrator and create accounts” on page 5](#)
- [“Supported browsers and JRE” on page 10](#)

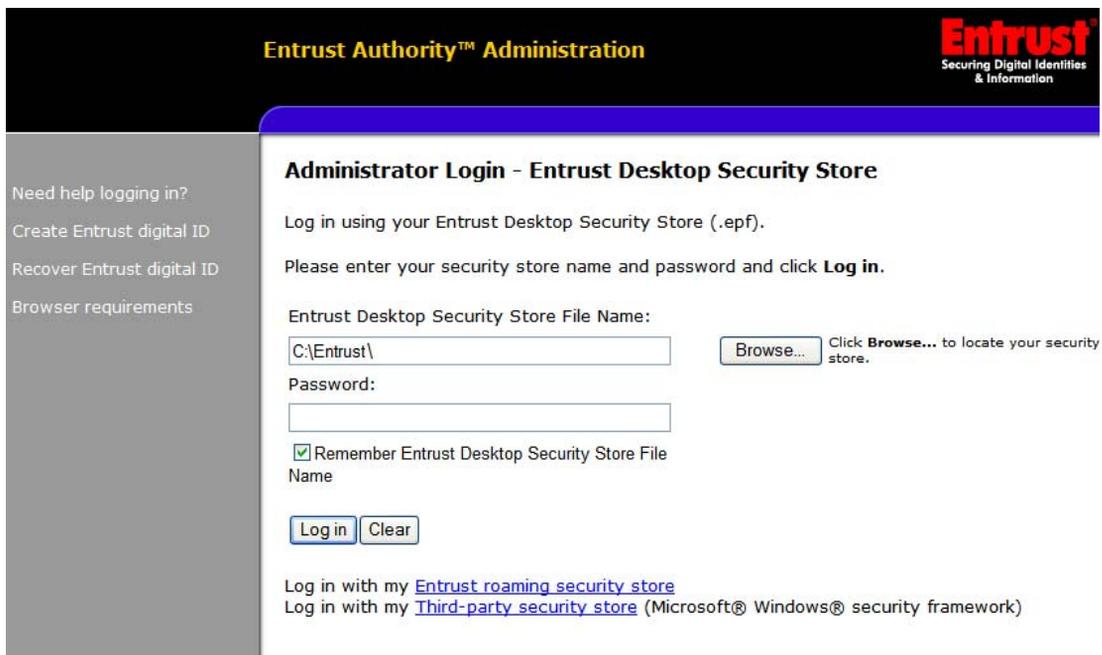
Creating an administrator digital ID

As an administrator accessing Administration Services for the first time, you need to add an administrator digital ID to a certificate store on your computer. Your digital ID is for your use only and cannot be applied to other users.

You access Administration Services over the Web. Before you start, ensure that you have a supported browser and Java runtime environment. See [“Supported browsers and JRE” on page 10](#) for details.

To access the Administration Services Web site, enter the URL provided with your Entrust Managed Services PKI welcome package.

The following page appears.



The screenshot shows the 'Entrust Authority™ Administration' web interface. The main heading is 'Administrator Login - Entrust Desktop Security Store'. Below this, there is a section for logging in using an Entrust Desktop Security Store (.epf) file. The form includes a text input for the 'Entrust Desktop Security Store File Name' (containing 'C:\Entrust\'), a 'Browse...' button, and a 'Password' field. A checkbox labeled 'Remember Entrust Desktop Security Store File Name' is checked. At the bottom of the form are 'Log in' and 'Clear' buttons. Below the form, there are two links: 'Log in with my [Entrust roaming security store](#)' and 'Log in with my [Third-party security store](#) (Microsoft® Windows® security framework)'. The Entrust logo is in the top right corner, and a left-hand menu contains links for 'Need help logging in?', 'Create Entrust digital ID', 'Recover Entrust digital ID', and 'Browser requirements'.

To enroll for your administrator digital ID, do the following:

- 1 Click **Create Entrust digital ID** in the left-hand menu.
The **Create Entrust Digital ID** page appears.

Entrust Authority™ Administration

Entrust
Securing Digital Identities
& Information

Need help creating your Entrust digital ID?
Return to the login page

☛ Create Entrust Digital ID

To create your Entrust digital ID, you have the following options:

- [Create Entrust Desktop Security Store](#)
Your digital ID will be stored in an Entrust desktop security store that is saved on your computer's hard drive.
- [Create Entrust Roaming Security Store](#)
Your digital ID will be stored in an Entrust roaming security store that is saved in your company's Directory.
- [Create Third-Party Security Store](#) managed by Entrust (Microsoft® Windows® security framework).
Your Entrust digital ID will be stored in the Microsoft® Windows® security framework certificate store located on your computer or on a smart card.

- 2** Click **Create Entrust Desktop Security Store** in the main pane.
The following page appears.

Entrust Authority™ Digital Identity Management

Entrust
Securing Digital Identities
& Information

[Home](#)

Need help?

☛ Create Entrust desktop security store.

To create your Entrust desktop security store, please enter the required information in the form below.

Entrust Desktop Security Store Name

Reference Number (for example: 27600839)

Authorization Code (for example: 6JIG-4LOV-OXLQ)

Password

Confirm Password

Password Rules

- ✓ must be at least 8 characters long
- ✓ must contain an uppercase character
- ✓ must contain a lowercase character
- ✓ must contain a numeric character
- ✓ must not contain a portion of the security store name longer than half its length
- ✓ must not repeat a character more than half the length of the password
- ✗ password and confirm password must match

- 3** To specify where you want to store the new profile on your computer, click **Browse**.
A dialog box appears.
- 4** Navigate to where you want to store your digital ID (also called a credential).
- 5** Provide a file name and ensure it has the extension `.epf`. Click **Open**.
- 6** On the **Create Entrust desktop security store** page, enter your administrator reference number and authorization code assigned to you as part of your Entrust Managed Services PKI welcome package.
- 7** Enter the password you want to use to protect your administrative profile. You will use this password to log in to Administration Services after you create your profile. Follow the on-screen password rules. The red X beside each rule changes to a green check mark as you type in characters that meet the rules.
- 8** Click **Create Security Store**.
You will see a message to wait while Administration Services creates the digital ID, followed by a success message.
You have now created your credential.
- 9** Click **Home** to return to the login page.

Log in as an administrator and create accounts

Once you create your administrator profile, you can use your digital ID to log in to the Administration Services portal.

If you are not already on the login page, enter the URL provided with your Entrust Managed Services PKI welcome package.

The screenshot shows the 'Entrust Authority™ Administration' interface. The main heading is 'Administrator Login - Entrust Desktop Security Store'. Below this, it says 'Log in using your Entrust Desktop Security Store (.epf). Please enter your security store name and password and click **Log in**.' There are two input fields: 'Entrust Desktop Security Store File Name:' with the value 'C:\Entrust\' and a 'Browse...' button. Below that is a 'Password:' field. A checkbox is checked with the label 'Remember Entrust Desktop Security Store File Name'. At the bottom of the form are 'Log in' and 'Clear' buttons. Below the form, there are two links: 'Log in with my [Entrust roaming security store](#)' and 'Log in with my [Third-party security store](#) (Microsoft® Windows® security framework)'. The top right corner features the Entrust logo with the tagline 'Securing Digital Identities & Information'. On the left side, there is a navigation menu with links: 'Need help logging in?', 'Create Entrust digital ID', 'Recover Entrust digital ID', and 'Browser requirements'.

On the login page, do the following:

- 1 Click **Browse** and navigate to the location where you stored your administrator digital ID.
- 2 Select your security store (.epf file) and click **Open**. The file name and path are automatically entered into the **Entrust Desktop Security Store File Name** field. (The path you enter here is retained for later use until changed.)
- 3 Enter the password you created earlier and click **Log in**.

Upon successful login, the following page appears.

The screenshot displays the Entrust Authority Administration interface. At the top, the page title is "Entrust Authority™ Administration" and the Entrust logo is visible in the top right corner. The user is logged in as "Administrator: demo" and has a "Log Out" link. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation menus for Home, Tasks, Search, Saved Searches, and Help. The main content area is organized into sections: "Request Tasks" (Approve Pending Requests), "Account Tasks" (Create Account, Create Accounts from File, Reset Account, Deactivate Account, Reactivate Account), and "Search" (Search Accounts, Search Requests). Each task includes a brief description and a "More information..." link.

From this page, you can perform various administrative tasks. This guide describes how to create a new user account. You can also reset a user's account if a password or digital ID is lost, and you can deactivate and reactivate accounts. For more information on these additional procedures, use the online help incorporated in the specific task page.

Creating user accounts

You must create a user account for each person who needs a digital ID. When you create a new user account, Administration Services generates a reference number and authorization code for that user. You then must give this number and code to the target user in a secure manner before they can enroll for their digital ID. The most secure approach is to send the reference number and authorization code separately using different secure methods.

Creating a user account

To create a new user account, do the following:

- 1 Click **Create Account** under **Account Tasks** in the main pane or under **Tasks** in the left-hand menu.

The initial **Create Account** page appears.

The screenshot shows the 'Create Account' page in the Entrust Authority Administration interface. The page title is 'Entrust Authority™ Administration' and the user is logged in as 'Administrator: demo'. The main content area is titled 'Create Account' and contains instructions: 'Select the user type and certificate type for the new account.' Below this are two required fields: 'User Type: *' with a dropdown menu set to 'Person', and 'Certificate Type: *' with a dropdown menu set to 'Web - Default'. A 'Submit' button is located below the fields. The left-hand navigation menu includes sections for Home, Tasks (with sub-items like Approve Pending Requests, Create Account, etc.), Search, Saved Searches, and Help.

- 2 Leave the value for the **User Type** field as **Person**.
- 3 In the **Certificate Type** drop-down list, select **Web – Default** or your company's specific Web certificate type, if one is set up for you.
- 4 Click **Submit**.

A second **Create Account** page appears where you provide the user's name and other information.

Entrust Authority™ Administration **Entrust**
Securing Digital Identities
& Information

Administrator: demo Log Out

Home

Tasks

- Approve Pending Requests
- Create Account
- Create Accounts from File
- Reset Account
- Deactivate Account
- Password Update
- Reactivate Account

Search

- Search Accounts
- Search Requests
- List Accounts
- List Requests

Saved Searches

- Edit Saved Searches

Help

- Documentation
- About
- Change Password

Create Account ? Help

Please enter the following information:
* Indicates required information.

User Information

First Name: *

Last Name: *

Serial Number:

Email:

Comment

Notification Email
 Enter an email address for account status notifications. If no email address is specified, no account status notifications will be sent.

Same as above email address

Group Membership *

Member of Example group only

Role *

Choose a role for this account:

Location *

Choose a Directory location for the account

Select the searchbase:

Enter a parent DN:

[Submit](#)

- 5 Fill in the **First Name** and **Last Name** fields.
- 6 Optionally, fill in the **Serial Number**, **Email**, and **Comment** fields.
If you include the user's email address in the **Email** field, Administration Services will send a confirmation message and reference code to that person.
- 7 Select the member option under **Group Membership**. (The name of your company replaces the word Example in the image above.)
- 8 Set **Role** to **End User**.
- 9 Under **Location**, specify where to add the user in the Administration Services LDAP directory. Click **Select the searchbase** and then select

your company name from the drop-down list. (An entry for your company was created in the directory when you signed up for Entrust Managed Services PKI.)

10 Click **Submit**.

The **Create Account – Complete** page appears. You have successfully created a user account.

Entrust Authority™ Administration

Administrator: demo

Create Account - Complete

You have created the following account:

Name	Group	Role	Status
James McLaughlin	Example	End User	New

Activation Codes

Securely distribute these codes to the account holder:

Name: cn=James McLaughlin,ou=Example,o=Entrust,c=US

Reference Number: 0393536

Authorization Code: BEC-ZOH8-6J7

Codes were created on: Thursday, March 06, 2008 8:45:35 AM

Codes will expire on: Thursday, March 20, 2008 9:45:35 AM

[Create Local Digital ID](#) Create Digital ID for this account that will be saved on this computer in an .epf file

[Create Roaming Digital ID](#) Create Digital ID for this account that will be saved in your company's Directory

[Create Third-Party Security Store](#) Create Digital ID for this account that will be saved in Microsoft Windows security store on this computer or on a smart card

This page lists the new user's reference number and authorization code. Record this information and store it in a secure manner. Securely provide this information to the new user.

Creating user accounts in batch

If your administrator account role includes the "Create accounts in batch from a file" permission, you will see the **Create Accounts from File** option under **Account Tasks** in the main pane or under **Tasks** in the left-hand menu. This lets you can add groups of new users in batch. This method requires an input file of precise construction and is recommended for experienced administrators only. See the *Entrust Authority Administration Services Administration Guide* for details.

Supported browsers and JRE

To access the Administration Services Web site, ensure that you are using one of the following browsers (or a later version) on a Microsoft® Windows® operating system: Microsoft® Internet Explorer 6.0, Mozilla® Firefox 1.5, Mozilla® 1.7.2 and 1.7.10, and Netscape® Navigator 8.0.

Entrust Authority Administration Services uses Entrust TruePass® technology to authenticate administrators. As a result, you must ensure that one of the following Java runtime environments (JRE) is installed, and that applicable browser settings are configured. With all supported Web browsers, you must allow cookies and enable both Java and JavaScript.

You can download the Sun JRE from the following site:

<http://www.java.com/download>.

Browser	Java Runtime Environment (JRE)	Setting Name	Setting
Microsoft Internet Explorer 6	Microsoft Java Virtual Machine (JVM), Sun JRE 1.4.1+ and 1.5.+	First-party cookies	Accept or Prompt
		Allow per-session cookies (not stored)	Enable or Prompt
		Active scripting	Enable or Prompt
		Scripting of Java applets	Enable or Prompt
		Third-party cookies	Block
Microsoft Internet Explorer 7	See Microsoft Internet Explorer 6		
Mozilla Firefox 1.5	Sun JRE 1.4.1+ and 1.5.+	Allow sites to set cookies	Enable
		Enable Java	Enable
		Enable JavaScript	Enable
		If pop-up blocker is enabled, allowed sites	Administration Services sites
Mozilla 1.7.2, 1.7.10	Sun JRE 1.4.2 and 1.5+	See Mozilla Firefox 1.5	
Netscape Navigator 8.0	Sun JRE 1.4.2 and 1.5+	Enable cookies	Enable
		Enable Java	Enable
		Enable JavaScript	Enable