



Securing Your Digital Life

Entrust Authority Administration Services 7.2 *Overview*

November, 2006

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

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION AND/OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A SPECIFIC PURPOSE.



Table of Contents

1 Administration Services 7.2 Overview	2
2 Policy-Based Operations.....	2
3 User Management Service	4
4 User Registration Service	5
5 Zero-footprint Digital ID Creation	7
6 E-Mail Notification.....	7
7 About Entrust	7

1 Administration Services 7.2 Overview

Entrust Authority Administration Services is an Administration and Registration portal designed to facilitate the deployment and lifecycle management for end-user and device Digital IDs issued by the Entrust Authority Security Manager 7.x CA.

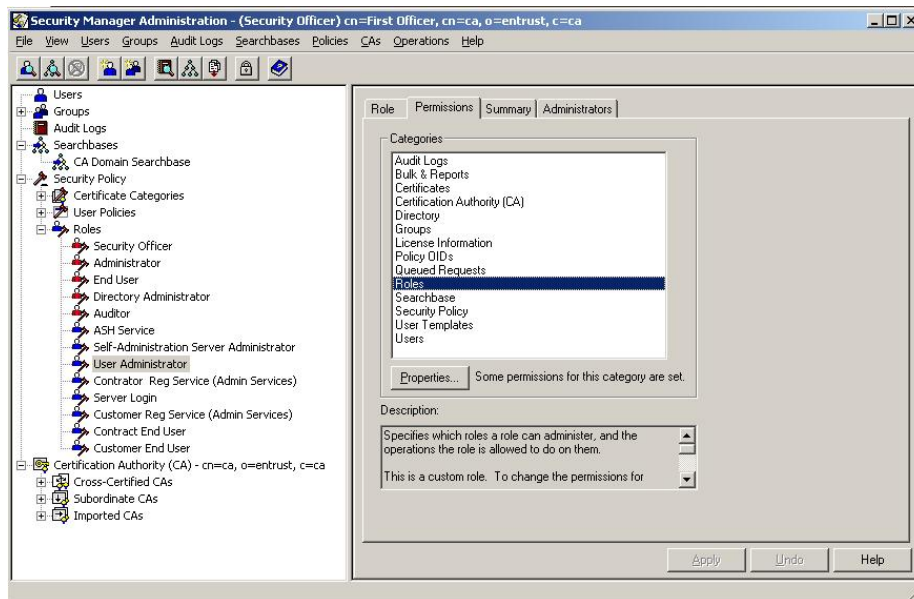
Entrust Authority Administration Services includes two web-based services/applications, a user-management service and a user-registration service, which all interact with Entrust Authority Security Manager 7.x to provide managed and browser-based Digital IDs.

Entrust Authority Auto-Enrollment Server, an optional integrated component, can also be added for even greater automation of lifecycle management of managed Digital IDs for end-users and “Local Machine” CryptoAPI (CAPI)-based Digital IDs specific to Microsoft desktops and servers.

The purpose of Administration Services is to deliver managed certificates to users for use with a wide range of enterprise applications such as file and folder protection, e-mail, e-forms, Wireless Local Area Network (WLAN) and Virtual Private Network (VPN) security.

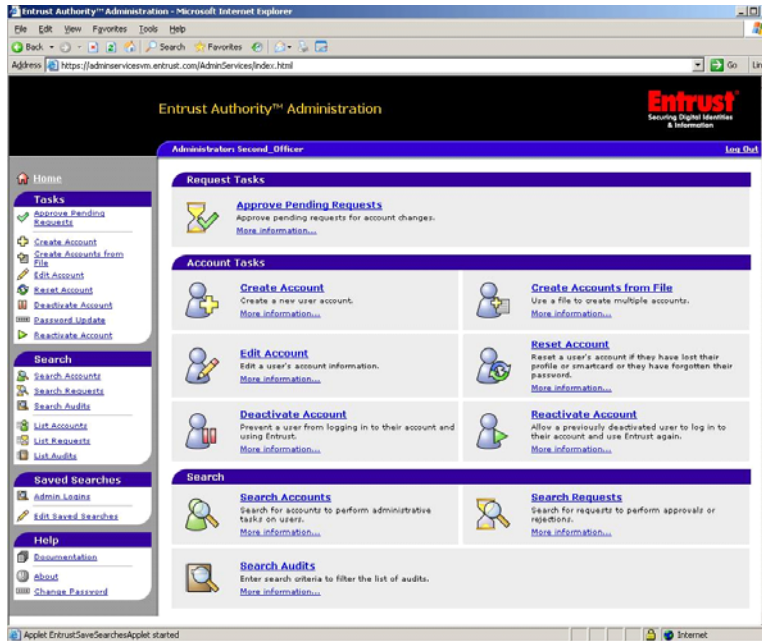
2 Policy-Based Operations

The operations of Local Registration Authorities (LRAs) via the User Management Service, or end-users via the User Registration Service, are controlled by administrative Roles and Permissions established centrally via the Registration Authority, Entrust Authority Security Manager Administration (SMA).

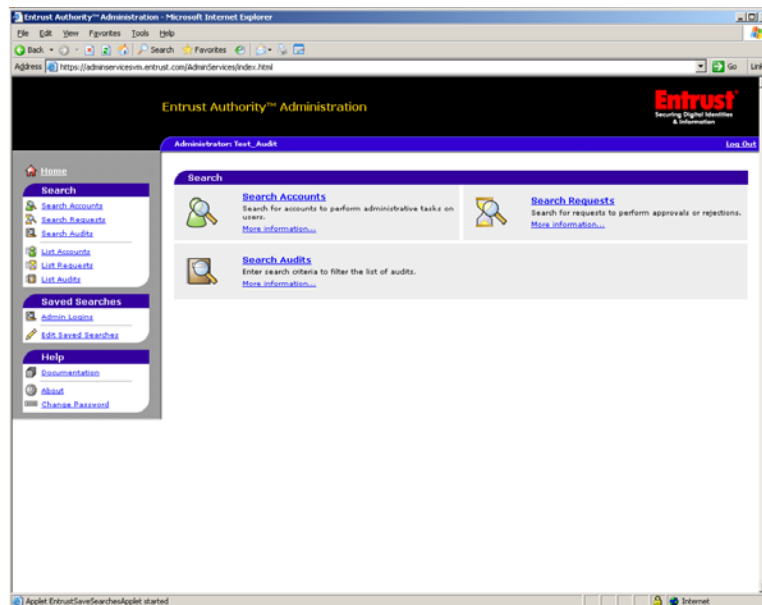


Entrust Authority Security Manager Administration User Interface showing permissions categories associated with a User Administrator role

Entrust Authority Security Manager Administration policy controls virtually every aspect of what administrators and users can see and accomplish via the Administration Services interfaces. Control is established at a role level so permissions can be adjusted efficiently for immediate and broad application against users, providing the granularity and separation to meet any business requirement. The administrative permissions are checked on every execution of a transaction to ensure that privilege levels are current.



The Administration Services User Management Interface as Displayed to a Fully Privileged LRA



The Administration Services User Management Interface as Displayed to a User with Audit Privileges Only

This approach allows for infinite flexibility in dealing with the distribution of administrative functions and the varying registration models, while maintaining strong centralized control over the processes that are at the foundation of the PKI trust model. The trust model is fully dependant on the level of assurance associated with the process that establishes the binding of the Digital ID to the end-user.

3 User Management Service

The User Management Service is the Web-based interface administrators use to perform administrative tasks. The service resides on a Web Server and Tomcat Application Server, and only grants access to administrators with the proper role, permissions and valid Entrust Digital ID.

The User Management Service is a standalone Web application that can run under its own J2EE Web application context. Multiple instances of the User Management Service — under different Web application contexts — may be deployed on a single servlet container (Tomcat) instance to manage differing configuration and branding requirements without imposing the need for additional hardware.

The User Management Service and User Registration Service instances may run concurrently within a single servlet container instance. The User Management Service has its own set of configurable settings for the E-mail Notification Service, separate from those of the User Registration Service.

The Web-based User Management Service application is accessed by an administrator to manage existing user accounts and process user requests in Security Manager 7.x. The User Management Service administrator may have the ability to perform the following tasks in the Web-based User Management Service application:

Account Tasks

- Creating accounts
- Creating accounts from a file — batch-user creation
- Editing accounts
- Resetting accounts
- Deactivating accounts
- Reactivating accounts
- Digital ID creation
- Digital ID recovery
- Managing saved searches

Request Tasks

- Manage pending requests
 - approve
 - cancel
 - delete

Search Tasks

- Searching accounts

- Searching requests
- Searching audits
- Saved search and audit criteria
- Listing accounts
- Listing requests
- Listing audits

Administrators employ Security Manager administrative credentials with an Entrust TruePass implementation that is integral to the User Management Service. The TruePass integration authenticates the administrator, as well as providing cryptographic services to sign all administrative transactions from the browser through the Entrust Authority Security Manager.

The Entrust Authority Administration application includes online help to guide administrators through the use of the application.

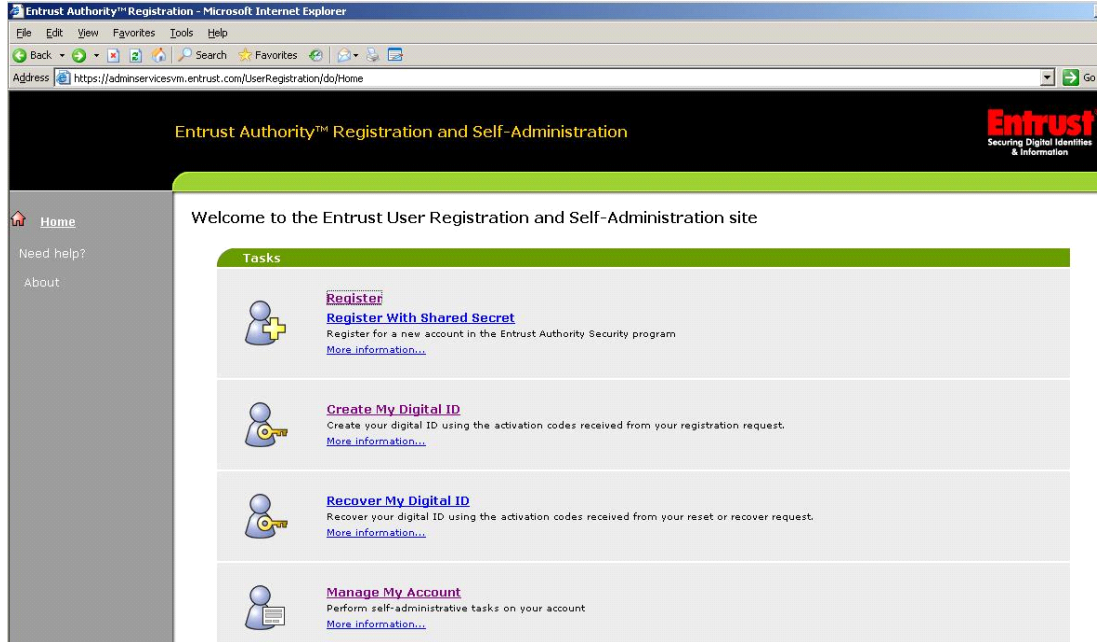
4 User Registration Service

The User Registration Service provides an interface for end-users to the self-registration and self-administration services provided by Security Manager. The Registration Servlet enforces Entrust Authority Security Manager policy as it pertains to the enrollment and self administration of end-users and Entrust Digital ID

The User Registration Service is a standalone Web application that can run under its own J2EE Web application context. Multiple instances of User Registration Service — under different Web application contexts — may be deployed on a single servlet container (Tomcat) instance.

The User Registration Service and User Management Service instances may run concurrently within a single servlet container instance. The User Registration Service can run on a server without the User Management Service. The User Registration Service has its own set of configurable settings for the E-mail Notification Service, separate from those of the User Management Service.

Much like the User Management Service, the User Registration Service tasks are controlled by configurable centralized policy. Each User Registration Service instance has a dedicated administrative role that controls every facet of the registration model for which it was deployed.



Entrust Authority Security User Registration User Interface Showing Available End-User-Initiated Operations

In addition, items such as the name of the product, branding and color scheme are customizable to reflect organizational requirements.

The end-user may have the ability to perform the following tasks in the User Registration Service:

- Registration
- Digital ID creation
- Digital ID recovery
- Management of the user's own account
 - Resetting an account
 - Revoking an account
 - Putting an account on hold
 - Removing hold from an account
 - Change Registration Password
 - Show Activation Codes

Once the user has created their Entrust Digital ID, it is used to encrypt, digitally sign and authenticate transactions. An Entrust Digital ID contains keys and certificates that can be used to verify one's identity.

The Entrust Authority Administration application includes online help to guide end-users through the use of the application.

5 Zero-footprint Digital ID Creation

Both the User Management Service and the User Registration Service deliver a zero-footprint Digital ID creation capability facilitating client-side key generation in a number of key store formats — including Entrust profile (.epf), Microsoft CAPI — or within the Entrust Roaming profile store. This approach allows organizations to provision Entrust Digital IDs without the need for client-side software.

6 E-Mail Notification

Entrust Authority Administration Services supports a task-driven, automated notification system. E-mail notification enables you to automatically send e-mail notification messages to administrators and users when specific events occur. The relevant information for the e-mail message is forwarded to the e-mail notification API from the User Management Service or User Registration Service, and the e-mail message is sent through an SMTP server. E-mail notification is enabled or disabled during the Administration Services installation

7 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries use Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services can help customers in achieving regulatory and corporate compliance, while helping to turn security challenges such as identity theft and email security into business opportunities. For more information on how Entrust can help secure your digital life, please visit: www.entrust.com