

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Technical Integration Guide for Red Hat Directory Server 7.1 and Entrust Authority Security Manager 7.1, Entrust Authority Roaming Server 6.0 and Entrust Entelligence Desktop Manager 7.0

July 2005

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. 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 REPRESENTATIONS AND/OR WARRANTIES 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, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Copyright © 2005. Entrust. All rights reserved.

Table Of Contents

Introduction	1
Entrust Product Information	1
Integration Overview	2
Integration Details	2
Preparing Schema files.....	2
Loading Schema into Directory.....	4
Configuring the Directory Server Instance.....	4
Configuring Entrust Products	5
Installing / Configuring Entrust Ready Products with Red Hat Directory Server:	5
System Behavior/Limitations	5
System Components	5
Partner Contact Information	6
Additional Information	6

Introduction

This technical integration brief provides an overview of how to integrate the following Entrust Ready products with Red Hat Directory Server:

1. Entrust Authority
 - a. Entrust Security Manager
 - b. Entrust Security Manager Administration
 - c. Entrust Roaming Server
2. Entrust Entelligence
 - a. Entrust Desktop Solutions

Integration with Red Hat Directory Server allows an organization to combine its Entrust PKI solution with the directory server designed and built by the inventors of LDAP. This mature, highly scalable product can be deployed with great flexibility to integrate diverse back end and legacy systems in a unified identity management solution.

Entrust Product Information

Entrust Authority™ Security Manager: The world's-leading public-key infrastructure (PKI), is designed to manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization.

As the organization's Certification Authority (CA) system, Entrust Authority Security Manager software enables the use of digital signature, digital receipt, encryption and permissions management services across a wide variety of applications and solutions.

Entrust Authority™ Administration Services: Administration Services is a web-based application that enables delegated and distributed administration of the Entrust Authority Security Manager PKI with end-to-end security by enforcing all administrative transactions to be digitally signed.

Entrust Authority™ Roaming Server: Roaming Server allows users to log in and have secure access to sensitive information – from any location – without having to carry the PKI digital IDs necessary to establish a secure connection.

Entrust Entelligence is based on:

Desktop Manager: a client application that provides a consistent, single security layer to the desktop, transparently and automatically managing digital IDs throughout their lifecycle on behalf of the user.

Security Provider: a thin client enterprise-wide desktop security platform that enables organizations to strongly authenticate users and add security, such as encryption and digital signatures, to their applications, in order to protect email and data using one single digital identity.

Partner Product Information

Partner Name: Red Hat, Inc

Website: <http://www.redhat.com>

Product Name: Red Hat Directory Server

Product Version: 7.1

Platform and Service pack: HP-UX 11i

Product description:

Red Hat Directory Server (formerly Netscape Directory Server) is a mature, highly scalable and reliable LDAP compliant server that centralizes application settings, user profiles, group data, policies, and access control information into a network-based registry.

A wide variety of business, education, and government organizations have deployed Red Hat Directory Server successfully to eliminate data redundancy and automate data maintenance. Red Hat Directory Server also improves security, enabling administrators to store certificates, policies, and access control information in the directory for a single authentication source across enterprise or extranet applications.

Integration Overview

Integration of Entrust Ready products with Red Hat Directory Server allows an organization to publish certificates to a highly scalable and reliable LDAP directory with proven performance.

Support for multi-master replication ensures that the directory deployment can be customized for maximum performance across geographically distributed organizations.

The Plug-In API provided by Red Hat Directory Server is especially useful for integrating diverse legacy applications or database backends within a comprehensive identity management solution.

A rich set of SDKs and tools also support rapid application development.

Integration Details

Integrating Entrust Ready products with Red Hat Directory Server involves the following steps.

1. Schema Preparation
2. Loading schema
3. Configuring Red Hat Directory Server
4. Installing/Configuring Entrust Ready Products

Preparing Schema files

The following 3 schema files need to be prepared in the format shown below.

1. pkcs9.ldif
2. 25rfc2587.ldif
3. entrust_schema.ldif

To comply with the pkcs9 specification, use the following pkcs9.ldif file.

```
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 1.2.840.113549.1.9.2 NAME 'unstructuredName' DESC 'PKCS #9 unstructured name'
EQUALITY caseIgnoreMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

attributeTypes: (1.2.840.113549.1.9.8 NAME 'unstructuredAddress' DESC 'PKCS #9 unstructured address' EQUALITY caseIgnoreMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

To comply with RFC 2587 , use the following 25rfc2587.ldif file.

```
dn: cn=schema
changetype: modify
add: objectClasses
objectClasses: ( pkiCA-oid NAME 'pkiCA' SUP top AUXILIARY MAY ( cACertificate
$ certificateRevocationList $ authorityRevocationList $ crossCertificatePair ) )
objectClasses: ( pkiUser-oid NAME 'pkiUser' SUP top AUXILIARY MAY userCertificate )
```

The following entrust_schema.ldif file is required by entrust ready products for LDAP integration.

```
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 1.2.840.113533.7.68.30 NAME ( 'entrustPolicyCertificate' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.22 NAME ( 'entrustRoamFileEnclInfo' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.28 NAME ( 'entrustRoamingEOP' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.24 NAME ( 'entrustRoamingPAB' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.23 NAME ( 'entrustRoamingProfile' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.27 NAME ( 'entrustRoamingPRV' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.25 NAME ( 'entrustRoamingRecipList' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.68.26 NAME ( 'entrustRoamingSLA' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( 1.2.840.113533.7.79.0 NAME ( 'entrustRoamingCAPAB' ) SYNTAX
1.3.6.1.4.1.1466.115.121.1.40 )
attributeTypes: ( email-oid NAME 'email' DESC 'email' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
-
add: objectClasses
objectClasses: ( 1.2.840.113533.7.67.17 NAME 'entrustPolicyObject' SUP top AUXILIARY MAY
entrustPolicyCertificate )
objectClasses: ( 1.2.840.113533.7.67.0 NAME 'entrustUser' SUP top AUXILIARY MAY userCertificate )
objectClasses: ( 1.2.840.113533.7.67.7 NAME 'rfc822MailUser' SUP top AUXILIARY MAY mail )
objectClasses: ( 1.2.840.113533.7.67.4 NAME 'uniquelyIdentifiedUser' SUP top AUXILIARY MUST
serialNumber )
objectClasses: ( 1.2.840.113533.7.67.5 NAME 'simpleAuthObject' SUP top AUXILIARY MUST
userPassword )
objectClasses: ( 1.2.840.113533.7.67.15 NAME 'entrustNamedObject' SUP top AUXILIARY MAY ( dc
$ cn $ sn $ c $ l $ st $ o $ ou $ title $ name $ givenName $ initials $ generationQualifier $ dmdName ) )
objectClasses: ( 1.2.840.113533.7.67.16 NAME 'uniquelyQualifiedObject' SUP top AUXILIARY MAY ( uid
$ mail $ serialNumber $ description $ dnQualifier ) )
objectClasses: ( 1.2.840.113533.7.67.13 NAME 'entrustRoamingUser' SUP top AUXILIARY MAY ( uid
$ entrustRoamFileEnclInfo $ entrustRoamingProfile $ entrustRoamingPAB $ entrustRoamingRecipList
$ entrustRoamingSLA $ entrustRoamingPRV $ entrustRoamingEOP $ entrustRoamingCAPAB ) )
```

```

objectClasses: ( 1.2.840.113533.7.67.12 NAME 'pKCS10Device' SUP top AUXILIARY MAY
serialNumber )
objectClasses: ( 1.2.840.113533.7.67.11 NAME 'cEPDevice' SUP top AUXILIARY MAY
( unstructuredName $ unstructuredAddress ) )
objectClasses: ( 1.2.840.113533.7.67.14 NAME 'entrustDNQualifierUser' SUP top AUXILIARY MAY
dnQualifier )
objectClasses: ( 1.2.840.113533.7.67.9 NAME 'emailAddressUser' SUP top AUXILIARY MAY email )

```

Loading Schema into Directory

Once the Idif files are prepared as shown above, use 'Red Hat Directory Server' specific ldap tools to load the schema into the directory server instance. An example is shown below:

```

ldapmodify -h <ldap_hostname> -p <ldap_port_number> -D "<directory_manager_dn>" -w
<directory_manager_password> -vf <full_path_to_schema_file>

```

Configuring the Directory Server Instance

Install Red Hat Directory Server as you would normally by following installation and instance setup instructions as explained in this document:

<http://www.redhat.com/docs/manuals/dir-server/install/7.1/installTOC.html>

Make sure that you allocate a new suffix under which all entrust related entries shall be created. Also make sure that the following entrust specific users are pre-created before you proceed with the Entrust Authority installation. Those entries would typically look like this:

```

# entry-id: 1
dn: cn=caauthority,ou=people,o=redhat
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationauthority
cn: caauthority
sn: caauthority
userpassword: <password_value>
cacertificate: <cert_value>
authorityrevocationlist: <value>
certificaterevocationlist: <value>

```

```

# entry-id: 2
dn: cn=admin,ou=people,o=redhat
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson

```

cn:admin
sn:admin
userpassword: <password_value>

Also make sure that the cn=admin user specified here has the proper ACI's (permissions) set on the suffix o=redhat so that it can read/write on the suffix.

Configuring Entrust Products

Installing / Configuring Entrust Ready Products with Red Hat Directory Server:

Please use the following documents to install and configure entrust products:

1. Install/Configure Entrust Authority Security Manager as you would normally by following the installation instructions as mentioned in this document :
 - a. https://www.entrust.com/trustedcare/documentation/proxy2.cfm/external/21567/SM_71_WIN_Install_2.pdf
2. Install/Configure Entrust Authority Security Manager Administration by following the installation instructions as mentioned in this document
 - a. https://www.entrust.com/trustedcare/documentation/proxy2.cfm/external/21564/SMA_71_Install_2.pdf
3. Install/Configure Entrust Authority Roaming server by following the installation instructions as mentioned in this document :
 - a. https://www.entrust.com/trustedcare/documentation/proxy2.cfm/external/1657/RS_60_Admin_Guide_Iss40.pdf
4. Install/Configure Entrust Entelligence Desktop solutions as mentioned in this document :
 - a. https://www.entrust.com/trustedcare/products/getall.cfm?level1=Entrust%20Entelligence&level2=Desktop%20Solutions&level3=Desktop%20Manager&level4=&category=doc&days=&version=7.0&language=english&external_only=false&internal_product=N

System Behavior/Limitations

No issues identified.

System Components

List Entrust products including their versions.	List Partner products including their versions.
Entrust Authority Security Manager --- 7.1	Red Hat Directory Server 7.1 on HP-UX 11i
Entrust Authority Security Manager Administration --- 7.1	
Entrust Authority Roaming Server --- 6.0	
Entrust Entelligence Desktop Solutions --- 7.0	

Partner Contact Information

Sales Contact:

Phone number: 1-866-273-3428 x45313

Online sales request:

https://www.redhat.com/apps/webform.html?event_type=contact_sales&eid=21

Support Contact:

Name: Neil Kruse

Address: 444 Castro Street. Mountain View, CA 94041

Telephone: 1-888-467-3342

Fax: 650 567-9041

Email: nss-support-list@redhat.com

Please check PSIC for the latest supported version information at:

<https://www.entrust.com/support/psic/index.cfm>

Additional Information

Business Contact Information

Name: Sean Cotter

Address: 444 Castro Street

Mountain View, CA 94041

USA

Email: ccotter@redhat.com

<http://www.redhat.com>

<http://www.redhat.com/software/rha/directory/>