Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Technical Integration Guide for Entrust Authority™ Security Manager 7.1 and IBM® Tivoli® Directory Server 6.0

March 2006

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

Partner Product Information 1

Integration Overview 2

Integration Details 2

- Configuring the Directory 2
- Schema Modifications 4
- Referral Configuration 4
- Cross Certification 4
- IBM Tivoli Directory Server Files 6

Configuring Entrust Authority™ Security Manager 8

System Behavior/Limitations 8

System Components 8

Partner Contact Information 8

© Copyright 2005 Entrust.
All rights reserved.

Introduction

This technical integration guide provides an overview of how to integrate Entrust Authority™ Security Manager 7.1 with IBM® Tivoli® Directory Server 6.0.

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.

Partner Product Information

Partner Name: International Business Machines (IBM)
Website: http://www-306.ibm.com/software/tivoli/products/directory-server
Product Name: IBM Tivoli Directory Server
Product Version: 6.0
Platform and Service Pack: Windows, AIX, Solaris, Linux, and HP-UX
For complete description of supported platform and system requirements please see
http://www-306.ibm.com/software/tivoli/products/directory-server/platforms.html

Product Description: The IBM Tivoli Directory Server implements the Internet Engineering Task Force (IETF) LDAP V3
specifications. It also includes enhancements added by IBM in functional and performance areas. This version uses IBM DB2 ® as the backing store to provide per LDAP operation transaction integrity, high performance operations, and on-line backup and restore capability. The IBM Tivoli Directory Server interoperates with the IETF LDAP V3 based
clients. Major features include:

- A Graphical User Interface (GUI) that can be used to administer and configure the IBM Tivoli Directory Server.
- A dynamically extensible directory schema
- UTF-8 (Universal Character Set Transformation Format)
- Simple Authentication and Security Layer (SASL)
- Replication
- Referrals
- Access control model
- Change Log
- Password policy
- Security audit logging
- Dynamic configuration changes using LDAP APIs

You will find more information at http://publib.boulder.ibm.com/tividd/td/IBMDirectoryServer6.0.html

© Copyright 2005 Entrust.
All rights reserved.

Integration Overview

This document covers the customization necessary to configure the IBM Tivoli Directory Server (TDS) v6.0 for use with Entrust Authority Security Manager v.7.1. Before starting the configuration of the Entrust with TDS products, these steps must be completed.

Integration Details

Configuring the Directory

In order to configure Entrust Authority Security Manager v.7.1 with IBM Tivoli Directory Server (TDS) v6.0, the entry for the Entrust CA must first be created, and a user entry must be added to the Entrust Authority Security Manager v.7 with the appropriate permissions defined. Create the suffix in IBM Tivoli Directory Server (TDS) v6.0 by logging in to the IBM Tivoli Directory Server (TDS) v6.0 Administrator GUI in your browser (Note that Web Application Server needs to be running before using GUI Administration tool for IBM Tivoli Directory configuration Tool http://directory_server_hostname:9080/IDSWebApp/IDSjsp/Login.jsp). Once you have logged in, expand the server administration -- >**Manage server properties** category in the navigation area of the Web Administration Tool, and select the **Suffixes** tab.
1. Enter the Suffix DN, for example, **o=ibm,c=us**. The maximum is 1000 characters for a suffix.

2. Click **Add**.

3. When you are finished, click **Apply** to save your changes without exiting, or click **OK** to apply your changes and exit, or click **Cancel** to exit this panel without making any changes.

4. Start IBM Tivoli Directory Server.

OR you can even use idsxcfg (IBM Tivoli Directory Server Configuration Tool) for creating suffix. Just follow below mentioned steps :

1. Start IBM Tivoli Directory Server Configuration Tool by executing *idsxcfg –I instancename* from a command window.
2. Select “Manage suffixes”.
3. Provide suffix DN in the “Suffix DN edit box” like o=ibm,c=us
4. Click add

Once you have added your suffix for the CA, you must then update IBM Tivoli Directory Server (TDS) v6.0 to add the suffix entry to the directory, and set the appropriate access rights. A sample LDIF file, ***V3.IBM.Entrust70.suffix.ldif***, is provided below. You must update this file to represent the directory structure you are creating. The sample assumes that the CA entry is being created at the suffix level. If your directory structure defines your CA entry below a suffix, then further customization will be required.
Within the sample file, you will need to make the following updates:

<*suffix*> - all occurrences of this value should be replaced with your suffix.
<*suffix-object-class*> - this value should be replaced with the directory object class you have used for your suffix.
<*suffix-object*> - this value should be replaced with the value of your suffix object.
<*cn=root*> - this value should be replaced with your directory server administrator id.
<*secret*> - this value should be replaced with the password you wish to use for your CA entry, and the administrator account for Entrust [LG: What product are referring to here?].
<*diradmin*> – this value should be replaced with the administrator id you wish to use for Entrust. Ensure you

© Copyright 2005 Entrust.
All rights reserved.

search for and replace all occurrences of diradmin (including ACL's).
The following diagram provides an example with the necessary updates. The Entrust CA is a suffix entry, *o=ibm, c=us*. The directory administrator id is the default, *cn=root*. The Entrust administrator id is *admin*, and we are using *entrust* for the CA password, and *entrustadmin* for the Entrust administrator id.

Updated V3.IBM.Entrust70.suffix.ldif file

```
# version: 1
dn: o=ibm,c=us
objectclass: top
objectclass: organization
objectclass: entrustCA
objectclass: pkiCA
objectclass: entrustUser
objectclass: emailAddressUser
objectclass: uniquelyQualifiedObject
objectclass: entrustPolicyObject
o: ibm
userPassword: entrust
aclentry: access-id:
o=ibm,c=us:object:ad:normal:rwsc:sensitive:rwsc:critical:rwsc
aclentry: access-id:
cn=admin,o=ibm,c=us:object:ad:normal:rwsc:sensitive:rwsc:critical:rwsc
aclentry:
group:CN=ANYBODY:normal:rsc:at.authorityRevocationList:rsc:at.crossC
ertificatePair:rsc:at.caCertificate:rsc:at.certificateRevocationList:rsc:at.
userCertificate:rsc
entryowner: access-id:o=ibm,c=us
entryowner: access-id:cn=root
ownerpropagate: TRUE
aclpropagate: TRUE
dn: cn=admin,o=ibm,c=us
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: entrustca
objectclass: entrustuser
objectclass: emailaddressuser
objectclass: uniquelyQualifiedObject
cn: admin
sn: Administrator
userPassword: entrustadmin
```

Once you have completed your updates, you need to load the LDIF file. Start **IBM Tivoli Directory Server Configuration Tool** GUI OR **IBM Tivoli Directory Server Configuration Tool**, click on the **Import LDIF data** on the left navigation pane. Enter the full path and file name on the import screen and click on ***Import***. Once the import completes, restart the directory server.

It is also possible to use the command line tools for this purpose. Make sure that the directory service is running and use **ldapmodify** (please make the appropriate edits to the *V3.IBM.Entrust71.at.ldif* file). As an example:

ldapmodify –a –h <hostname> -p <ldapport> -D "cn=root" –w <password> -i <filename>

© Copyright 2005 Entrust.
All rights reserved.

Please note, if the ldif file is not in the current working directory, provide the full path and file specification.

Schema Modifications

Entrust Authority Security Manager v.7.1 requires certain directory attributes that are not provided by default with IBM Tivoli Directory Server (TDS) v6.0. To add the necessary schema, download the IBM Tivoli Directory Server (TDS) V6.0 and Entrust Authority Security Manager v.7.1 schema updates from:
http://www-1.ibm.com/support/docview.wss?rs=767&context=SSVJJU&dc=DB520&dc=D600&dc=DB530&dc=D700&dc=DB500&dc=DB540&dc=DB510&dc=DB550&q1=1236557&uid=swg21236557&loc=en_US&cs=utf-8&lang=en

There will be three files to download: *Entrust.doc, EntrustSample.ldif and EntrustSchemaldif.ldif.* *EntrustSchemaldif.ldif* is actually the ldif file that contains required attribute and object class modifications. Other two files are provided to expedite the CA configuration as *entrust.doc* reiterates the steps to configure the CA and *EntrustSample.ldif* is a sample file with appropriate user and access rights defined.

Once you have downloaded the files, you will need to update your directory server to include the schema updates.

Note: If you are using multiple directory servers, these updates must be loaded into all directory servers.
To add the Entrust Authority Security Manager v.7 schema updates to IBM Tivoli Directory Server (TDS) v6.0 from a command line, use the *ldapmodify* command:
ldapmodify –h *directory_server_host_name* –p *port* –D *directory_administrator_id* –w *directory_administrator_password* –i */file_path/file_name*
directory_server_host_name – this is the fully qualified DNS name of your directory server.
port – the port number you have configured for the TDS server. The default port number is 389. If you have changed the default port, you must specify this parameter.
directory_administrator_id – this is the id of the TDS administrator.
directory_administrator_password - this is the password of the TDS administrator.
/file_path – the path to the location where you have stored the Entrust schema updates.
/file_name – the name of the Entrust schema updated files.

Referral Configuration

Configuration was achieved per the on-line IBM Tivoli Directory Server (TDS) v6.0 documentation. Check IBM Tivoli Directory Server (TDS) v6.0 administration guide, for details.

Following are the brief steps that could help configuring referral between directories that are to be used for cross certifications.

Cross Certification

Following are the steps that need to be carried out to enable EASM for cross certification among different C.A.s

Base Setup:

Configure CA in a windows machine where EASM is already installed. To do this follow the steps mentioned below (Preparing directory for Entrust).

Say 1st configured CA is o=ibm,c=us in say machine M1.

© Copyright 2005 Entrust.
All rights reserved.

Configure CA in second windows machine say as o=ibmIndia,c=India.

MAKE SURE THE TWO WINDOWS MACHINES HOSTING EASM ARE SYNCHRONIZED WITH RESPECT TO TIME/TIME ZONE.

Both the machines having Entrust Security Manager must have Entrust Security Administrator (ESA) installed also!

Now update directories associated with both the EASM in order to have referral of each other set in the directories.

Base Setup Steps:

Create Suffixes for another CA in the directory associated with CA. To do so follow these steps:

1. Stop Directory Server associated with CA1 by executing ibmslapd command.
   Ibmslapd –I inst1 –k
 (Where inst1 is the instances created for hosting Entrust CA 1.)
2. Add suffix of second CA DN i.e o=ibmIndia,c=India.
   Idscfgsuf –I inst1 –s “o=ibmIndia, c=India” -n
3. Start the Server.
   Ibmslapd –I inst1 -n

Add following referral entry in the First CA (o=ibm,c=us)

```
ldapadd –h hostname –D cn=root –w rootpassword
dn: o=ibmIndia,c=India
ref:ldap://hostname_of_other_CA/o=ibmIndia,c=India
objectclass:referral
```

Similarly create suffix and add referral to CA 2 o=ibmIndia, c=India for CA 1 as follows:

1. Stop Directory Server associated with CA 2 by executing ibmslapd command.
   Ibmslapd –I inst1 –k
 (Where inst1 is the instances created for hosting Entrust CA 2.)
2. Add suffix of second CA DN i.e o=ibmIndia,c=India.
   Idscfgsuf –I inst1 –s “o=ibm, c=us” -n
3. Start the Server.
   Ibmslapd –I inst1 -n
4. Add following referral entry in the Second CA (o=ibmIndia,c=India)
   ldapadd –h hostname –D cn=root –w rootpassword
   dn: o=ibm,c=us
   ref:ldap://hostname_of_other_CA/o=ibm,c=us
   objectclass:referral

Make sure both directories are reachable to each other using ldapsearch.
Ldapsearch –h “CA 1 Host” –D cn=root –w rootpassword –s base –b “o=ibmindia,c=india” objectclass=*

It should show the results from other CA i.e CA 2.

Similarly, ldapsearch in second CA i.e. CA 2 for first CA i.e. CA 1
Ldapsearch –h “CA 2 Host” –D cn=root –w rootpassword –s base –b “o=ibm,c=us” objectclass=* , should show results for CA 1.

© Copyright 2005 Entrust.
All rights reserved.

Now follow the steps mentioned below for cross certification:

Steps To Prepare Cross Certification:

1. Login to ESA on first CA say CA1 with security officer's credentials.
2. Expand Certification Authority control in the ESA.
3. Select Cross Certified CAs, and right click on mouse.
4. Select Online Cross Certification -> Begin Online Cross Certification.
5. Provide DN of the CA whom you want to establish Cross Certification.
6. Select Default Cross – Certificate In Certificate Info Tab.
7. Select Mutual as cross certification type.
8. Click ok; validate it by providing First Officer's password.
9. Now refresh the Cross Certified CAs tab and see the Cross Certification Password is generated and Cross Certified CA status is shown as pending.
10. Login to ESA on second CA i.e. CA2 with security officer's credentials.
11. Expand Certification Authority control in the ESA.
12. Select Cross Certified CAs, and right click on mouse.
13. Select Online Cross Certification ->-Complete Online Cross Certification.
14. Provide the password generated in the CA 1 here. Provide DN of CA 1 and port is by default the port, which EASM opens. Select the default Certificate type and keep it mutual i.e. same as asked for, by CA 1.
15. If everything goes ok Cross Certification completes and status shown in both CA 1 and CA2 is "complete".

IBM Tivoli Directory Server Files

V3.IBM.Entrust71.at.ldif

```
# Attribute file for IBM Tivoli Directory Server V6.0
# Entrust V7.1
# Dependencies:
#
dn:cn=schema
changetype: modify
add: attributetypes
attributetypes: (

2.5.4.58
```

© Copyright 2005 Entrust.
All rights reserved.

```
NAME 'attributeCertificateAttribute'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
USAGE userApplications
)
ibmattributetypes: (
2.5.4.58
DBNAME( 'attriCertattr' 'attriCertattr' )
ACCESS-CLASS normal
)
```

V3.IBM.Entrust71.oc.ldif

```
# Objectclass file for IBM Tivoli Directory Server V6.0
# Entrust V7.1
# Dependencies:
#
dn:cn=schema
changetype: modify
replace: objectclasses
objectclasses: (
2.5.6.24
NAME 'pmiUser'
DESC 'pmiUser for Entrust/PKI 5.1'
SUP top
AUXILIARY
MAY ( attributeCertificate $ attributeCertificateAttribute )
)
```

V3.IBM.Entrust71.suffix.ldif

```
# version: 1
dn: <suffix>
objectclass: top
objectclass: organization
objectclass: entrustCA
objectclass: pkiCA
objectclass: entrustUser
objectclass: emailAddressUser
objectclass: uniquelyQualifiedObject
objectclass: entrustPolicyObject
<suffix-object-class>: <suffix-object>
userPassword: secret
aclentry: access-id:<
suffix>:object:ad:normal:rwsc:sensitive:rwsc:critical:rwsc
aclentry: access-id:
cn=diradmin,<suffix>:object:ad:normal:rwsc:sensitive:rwsc:critical:rwsc
aclentry:
group:CN=ANYBODY:normal:rsc:at.authorityRevocationList:rsc:at.crossC

ertificatePair:rsc:at.caCertificate:rsc:at.certificateRevocationList:rsc:at.
userCertificate:rsc
entryowner: access-id:<suffix>
entryowner: access-id:cn=root
ownerpropagate: TRUE
aclpropagate: TRUE
dn: cn=diradmin, <suffix>
objectclass: inetOrgPerson
```

© Copyright 2005 Entrust.
All rights reserved.

objectclass: organizationalPerson
objectclass: person
objectclass: entrustca
objectclass: entrustuser
objectclass: emailaddressuser
objectclass: uniquelyQualifiedObject
cn: diradmin
sn: Administrator
userPassword: secret

Configuring Entrust Authority™ Security Manager

Please see "Configuring the Directory" section above.

System Behavior/Limitations

None known.

System Components

Entrust Authority Security Manager 7.1 IBM Tivoli Directory Server 6.0

Partner Contact Information

Sales and Support Contact: Keith Sams / Ph: 512-426-8109 /Fax: 845-491-3309
e-mail: ksams@us.ibm.com
http://www.ibm.com/software/tivoli/features/idmgmt/
Web: http://www.developer.ibm.com/
Please check PSIC for the latest supported version information at:
https://www.entrust.com/support/psic/index.cfm
Additional Information:
http://publib.boulder.ibm.com/tividd/td/IBMDirectoryServer6.0.html

© Copyright 2005 Entrust.
All rights reserved.