CA Directory

Integration Guide

r12.0 SP8

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Character Limitations and Special Characters

CA Directory requires that the names of computers, users, directories, and so on, are valid for the operating system and also adhere to the following restrictions:

- **Installation Location for CA Directory ($DXHOME or %DXHOME%)**—The name of the location (folder or directory) that CA Directory is installed into must contain only alphabetic and numeric characters.
- **DXlink Password in the Knowledge File (ldap-dsa-password)**—If the password that you specify for *ldap-dsa-password* in the knowledge file contains a backslash (\), you must escape it with a second backslash (\\).

  For example, if the actual password is *p3.M\b@)*, you must include it in the knowledge file like this:

  ```
  ldap-dsa-password = "p3.M\\b@)"
  ```

- **Other Character Limitations**—CA Directory requires that the following items include only the standard ASCII characters that appear in English:
  - DSA names
  - Directory prefixes, for example, <c AU><o DEMOCORP>

Command Formatting Conventions

In this guide, commands are shown in a different font from the main text, as in this example:

```
get dynamic-group;
```

Variables that you must replace appear in italic text. In this example, replace *assoc-number* with the actual association number:

```
abort user assoc-number;
```

If you must enter only one of a list of options, the options are shown separated by the pipe character |. In this example, you should choose *either* true *or* false:

```
set access-controls = true | false;
```

Optional items are shown enclosed in square brackets, as the *tag* option is in this example:

```
set admin-user [tag] = own-entry
```

If items can be repeated, this is shown by a trailing ellipsis ..., for example:

```
item 1 [,item 2 ...]
```

File Location Convention

This document refers to the CA Directory installation location as DXHOME. For example, the location DXHOME/config/schema represents the following locations in a default installation:

- **Windows—**C:\Program Files\CA\Directory\dxserver**\config\schema**
- **UNIX—**/opt/CA/Directory/dxserver**/config/schema**

Format of Distinguished Names

The X.500 and LDAP communities differ in the way they write distinguished names (DNs):

- **X.500**—DNs are written from the top of the tree down, for example:

  ```
  <c US><o Acme><ou Staff><cn "John Citizen">
  ```

- **LDAP**—DNs are written from the leaf entry up, for example:

  ```
  cn=John Citizen, ou=Staff, o=Acme, c=US
  ```

If a portion of prefix is more than one word, you can enclose the whole prefix in quotes or just the problem portion. For example, both of these prefixes will work:

```
o=“democorp test”,c=au
“o=democorp test,c=au”
```

Note: Use a pair of quotes (“”) for a null DN.

Contents

Chapter 1: Integrate an Eracom HSM

This section discusses Windows only.

It has been tested on the following:

- ProtectServer Orange External (PSO-E)
- ProtectToolkit C Release 3.24 or higher

This section contains the following topics:

Examples in This Section

The examples here use the following settings:

- HSM hostname: **orange**.
- HSM IP address: **10.1.1.100**
- Gateway: **10.1.1.1**
- Subnet mask: **255.255.255.0**
- DNS IP address: **10.1.2.102**

The instructions are based on the sample directories provided with CA Directory. These sample directories include:

- The Democorp DSA
- The UNSPSC DSA

Configure the HSM

Log In to the HSM

The operating system of the Eracom HSM is based on Linux.

When you log in for the first time, the Eracom system prompts you for a new root password. Enter a password that is suitable for your company's security policy.

Confirm the HSM Initial State

To determine that the HSM is functioning correctly, enter the following command at the HSM root prompt:

```
hsmstate
```

If the HSM is functioning correctly, the system responds with the following message.

```
HSM device 0: HSM in NORMAL MODE. RESPONDING
```

Update the HSM Configuration Files

Before editing any files, back up the configuration files.

Set the HSM Hostname

To change the hostname on the HSM

1. Open /etc/hostname.

   This file contains only one line.

2. Change the line from the default of *rasam* to the HSM hostname. For example, change it to orange.

3. Save the file.

   This change will take effect when you restart the HSM.

Set HSM IP Address

To set the HSM IP address

1. Open the /etc/network/dualnet configuration file.
2. Change the following items:

```
# First Ethernet address
IP0 = 10.1.1.100
# Second Ethernet address
IP1 = 192.168.2.212
# Netmask
NETMASK = 255.255.255.0
# Network
NET1 = 10.1.1.0/24
# Gateway
GATEWAY = 10.1.1.1
```

3. Save the file.

Enable Name Resolution

To enable the HSM to resolve DNS names within your environment

1. Open the /etc/resolv.conf file.
2. Add the IP address of your DNS server:

```
nameserver 10.1.2.102
search gc.eracom-tech.com
```

Update the Active IP Tables

Access controls on the ProtectServer Orange External is performed using IP tables.

In the following example, the desired access control configuration is to deny access to all but one IP address, that of your directory host. In this example, the directory host's IP address will be 10.1.3.10.

```
iptables -F INPUT
iptables -A INPUT -s 10.1.3.10 -j ACCEPT
iptables -A INPUT -j DROP
/etc/init.d/iptables save active
```

Once the last command is entered, the HSM should respond with the following message.

```
Saving iptables ruleset: save “active” with counters
Please refer to the ProtectServer Orange External installation guide for further
details on the commands used.
```

Update the Inactive IP Tables

Before the IP tables are completely configured, it should have an inactive table defined. This is less critical as there is very little running in the operating system by the time the inactive table is loaded. The following set of commands provides you with a suitable inactive table.

```
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP
/etc/init.d/iptables save inactive
```

Once the last command is entered, the HSM should respond with the following message.

```
Savinging iptables ruleset: save “inactive” with counters
```

Restart Networking After Changes

After making and changes to the networking configuration, reboot the HSM or restart the networking with the following command:

```
/etc/init.d/networking restart
```

Install the Eracom Win32 Software

For the best performance, and to ensure communications between the directory server and the Eracom HSM, it is best to install both the Network Access Provider and Protect ToolkitC on the directory server itself.

Install The Network Access Provider

To install the Win32 Network Access Provider onto the directory host

1. Insert the CD **ProtectToolkit C Orange** into the CDROM drive of the directory host.
2. Install the following package:

   ```
   {CDROM}:\Win32\Network_HSM_Access_Provider\ETnethsm.exe
   ```
3. At the Eracom Network HSM Access Provider Installation screen, click Next.
4. At the licence agreement screen, click Yes.
5. Choose your destination folder, and then click Next.

6. In the Remote Client Setup page, enter the IP address of the HSM ProtectServer Orange External HSM, and the listener TCP port. By default it is **12396.** Once you are complete, click Next.
7. Click Yes to update the path:
8. At the Setup Complete screen, click Finish.

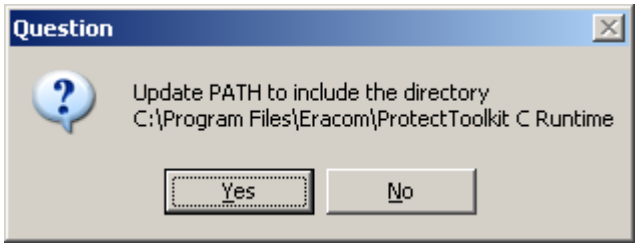
Install The Protect Toolkit C Runtime

To install the Win32 Protect ToolKit C Runtime onto the directory host

1. Insert the CD titled: ProtectToolkit C Orange into the CDROM drive of the directory host.
2. Install the following package:

   ```
   {CDROM}:\Win32\PTKC_Runtime\ETcprt.exe
   ```

   ```
   At the ProtectToolkit C Runtime Installation screen, click Next.
   ```
3. At the licence agreement screen, click Yes.
4. Choose your destination folder, and then click Next.
5. Click Yes to update the path:



6. At the Setup Complete screen, click Finish.

Confirm Software Installation

After the installation of the two packages, you should be able to confirm installation of the Eracom client utilities.

To confirm that the Eracom client utilities were installed

1. Open a command prompt
2. At the command prompt, enter in the following command:

   ```
   hsmstate
   ```

   The following output appears:

   ```
   hsmstate
   HSM device 0:   HSM in NORMAL MODE. RESPONDING
   ```

3. Enter the following command:

   ```
   ctconf
   ```

   The first time you run this command you will be asked to set the pin for two roles, Admin and Administrator.

   Select pins for both roles.

4. Enter the *ctconf* command again.

   The following output appears, demonstrating that the client utilities installed on the directory host are communicating with the Eracom HSM:

   ```
   ProtectToolkit C Configuration Utility $Revision: 1.129 $
   Copyright (c) Eracom Technologies 2003
   Current Adapter Configuration for Device 0:
   Model             : 8000:PL450
   Serial Number     : 4133
   Adapter Clock     : 15/06/2006 02:40:26 (+10:00)
   Battery Status    : GOOD
   Security Mode     : Default (No flags set)
   Transport Mode    : None
   FM Support        : Enabled
   FM Status         : No FM downloaded yet
   Open Session Count: 0
   Number of Slots   : 1
   RTC Adjustment Access Control: Disabled
   PLEASE NOTE that the firmware allows FMs to be downloaded; but the "Tamper before
   upgrade" security flag is not set. To protect existing keys against a possible
   threat of a rogue FM, this flag should be set (using 'ctconf -ft')
   ```

Create Certificates

To use the HSM, you need to create certificates.

Create A New Slot for the Certificates

To create a new slot for the certificates

1. Open a command window on the directory host and enter the following command:

   ```
   ctconf -c1
   ```

   This command requests the administrator's PIN.

2. Enter the PIN.

   In this example, set the PIN to 1000 on the test HSM.

   Once the administrator's pin is entered, the new slot will be created.

Test the New Slot

To test the new slot

1. Query the status of the slot using the following command:

   ```
   ctstat -sslot-number
   ```

   This produces output similar to this:

   ```
   ProtectToolkit C Status Utility $Revision: 1.32 $
   Copyright (c) Eracom Technologies 2003
   Slot ID 2
       Description      : CSA8000:53551
       Manufacturer     : ERACOM Pty. Ltd.
       Hardware Version : 71.00
       Firmware Version : 1.42
   Token for Slot ID 2
       Label            :
       Manufacturer     : ERACOM Pty. Ltd.
       Model            : 8000:PL450
       Serial Number    : 4133:53551
       Hardware Version : 71.00
       Firmware Version : 1.42
   ```

2. Look for the following message:

   ```
   ctcert: The token in slot # is not initialised.
   ```

   If you see it, run the following command:

   ```
   ctconf -nslot-number
   ```

3. Look for the following message:

   ```
   ctcert: The user PINN for the token in slot # is not initialised.
   ```

   If you see it, run the following command:

   ```
   ctkmu p -sslot-number
   ```

Generate the Certificate Authority Key Pair

To create the PEM certificates for the sample DSAs, you need to create a certificate authority, or CA. Create the certificate authority's key pair in the new slot.

To generate the certificate authority key pair

1. Enter the following command.

   ```
   ctcert c -k -lrootCA -sslot-number
   ```

2. Enter the user PIN for the slot.
3. Enter the following information about the certificate:
   - Common Name
   - Organization
   - Organizational Unit
   - Locality
   - State
   - Country

   This creates a CA keypair called **rootCA**. The output looks like this:

   ```
   ProtectToolkit C Certificate Utility $Revision: 1.52 $
   Copyright (c) Eracom Technologies 2003
   Enter user PIN for <Slot 2> DocoTest:
   Please enter the Subject DN for the key pair and certificate.
   Common Name: RootCA
   Organization: CA
   Organizational Unit: Labs
   Locality: Mooroolbark
   State: VIC
   Country: AU
   Generating new key pair, please wait...
   Creating certificate for 'rootCA'
   Issuer: 'CN=RootCA,O=CA,OU=Labs,L=Mooroolbark,ST=VIC,C=AU'
   Subject: 'CN=RootCA,O=CA,OU=Labs,L=Mooroolbark,ST=VIC,C=AU'
   ctcert: Certificate generated
   ```

Generate the DSA Certificates

You must now create the individual DSA personality certificates. Each of these certificates will be signed by the root CA certificate authority.

Each of the DSA certificates will be stored in slot 2, along with the CA certificate.

For this example, use the table below when entering the responses:

DSA Name	Certificate Distinguished Name Attributes
Democorp-Master-democorp	cn=DXServer,o=Democorp,c=AU
UNSPSC-Master-unspsc	cn=DXServer,o=UNSPSC,c=AU
Router-Master	cn=DXServer,c=AU

To generate the DSA certificates

1. Enter the following command:

   ```
   ctcert c -crootCA -k -ldsa-name -s2
   ```

2. Enter the user PIN for the slot.
3. Enter the following information about the certificate:
   - Common Name
   - Organization
   - Country

   Leave any other fields blank.
4. Repeat for each of the DSAs that are required.

Test the New Certificate

You should now check that you created the certificates correctly.

To list the certs in slot number 2, enter the following command:

```
ctcert l -s2
```

Export the CA Certificate to a PEM File

Before you can configure the DXserver to work with the HSM, you must export the root CA and DSA certificates to PEM files.

Note: Only the certificates will be exported, not the private keys. The private keys will remain in the HSM.

To export the CA certificate

1. Change to the **ssld** directory
2. Export the certificate, using the following command:

   ```
   ctcert x -frootCA.pem -s2 -lrootCA
   ```

   where:

   -l***certificate-lable***

   Specifies the label of the certificate stored in the HSM slot

   -f***filename***

   Specifies the file name of the exported certificate

Export the DSA Certificates to PEM Files

The command to export the DSA certificates is exactly the same as the command used in the previous topic, except the DSA names replaces the *rootCA* values.

To export the DSA certificates

1. Change to the **ssld\personalities** directory.
2. Export the certificates, using the following commands:

   ```
   ctcert x -fDemocorp-Master-democorp.pem -s2 -lDemocorp-Master-democorp
   ctcert x -fUNSPSC-Master-unspsc.pem -s2 -lUNSPSC-Master-unspsc
   ctcert x -fRouter-Master.pem -s2 -lRouter-Master
   ```

   -l*certificate-label*

   Specifies the label of the certificate stored in the HSM slot.

   -f*filename*

   Specifies the file name of the exported certificate.

Change the DSA Configuration to Use the New Certificates

You must now configure each individual DSA to use HSM certificates.

To change the DSA configuration to use the new certificates

1. Create an SSLD configuration file with the following content:

```
# HSM configuration
set ssl = {
    cert-dir = "config/ssld/personalities"
    ca-file = "config/ssld/rootCA.pem"
    pin = "1000"
    lib = "C:\Program Files\Eracom\ProtectToolkit C Runtime\cryptoki.dll"
    slot = 2
};
```

2. Save this new file as config\ssld\HSM.dxc.
3. Modify the DXI file to use the new SSLD configuration file:
   a. Find the following line:

```
source "../ssld/default.dxc";
```

   b. Replace it with this line:

```
source "../ssld/HSM.dxc";
```

4. Restart all DSAs.

Test Whether SSL Is Working

This section presents the following ways to test whether the SSL functionality is working:

- Use an LDAP browser to connect to the DSA using SSL.
- Use LDAP tracing to trace incoming and outgoing operations.

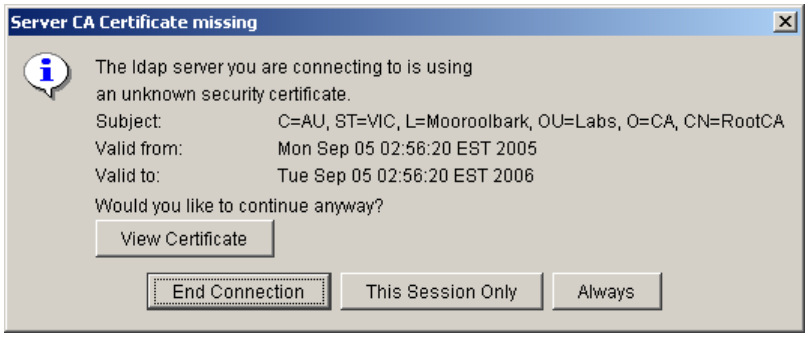
Connect To The Directory Using SSL

You should now connect to the directory using SSL, to confirm the SSL functionality. You can use an LDAP browser such as JXplorer.

To test the SSL functionality

1. Use an LDAP browser to connect to the router DSA, using the following details:
   - DSA name: Router-Master
   - Port: 19289
   - Authentication level: SSL + anonymous.
   - Base DN: blank

   When the connection is established, a dialog appears, similar to the following:



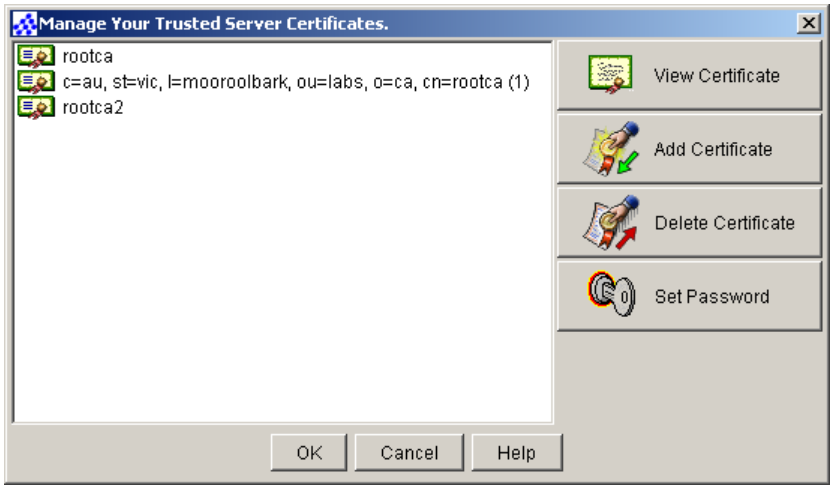
   This confirms your trust of the trusted root certificate that has been presented to the LDAP browser.

2. To trust the certificate and add it to the trusted certificate key store of the JXplorer browser, click Always.

   This connection validates that CA Directory is communicating with HSM.

3. Confirm the certificate has been loaded into the keystore of the browser. To do this in JXplorer, click on the Security menu, and select Trusted servers and CAs.

   This opens a lists of the certificates registered in the keystore.



   Because the root CA is trusted by the browser, any DSA that presents a certificate signed by this root CA is immediately trusted by your browser.

Trace Incoming and Outgoing Operations

To prove the SSL communications in another way, you can trace (with a trace setting of LDAP) the router DSA.

If SSL is working, the incoming and outgoing operations are preceded by the text *(SSL)*.

Chapter 2: Integrate a Websphere Portal Server

This section discusses Windows only.

It has been tested on Websphere Portal Server 5.1.0.1 and 6.0.

This section contains the following topics:

Install CA Directory

To install CA Directory

1. Use the Installation Guide for instructions on installing CA Directory.
2. Insert the CA Directory CD, or download the latest version from http://ca.com/support.
3. Install the following packages:
   - Directory
   - Directory Management

     You only need to install the JXweb component from this package.

Create a CA Directory Backbone

You need to create a new DSA to store the user entries that Websphere Portal Server and Websphere Application Server require.

Use DXmanager to create a new backbone that includes a single DSA, and make sure that the DSA is started.

Populate CA Directory

Before you install and configure Websphere Portal & Application Servers, you must have a default set of user accounts and groups populated in the directory.

This section describes how to create LDIF files containing the necessary users and groups, and how to load them into the DSA.

The LDIF data in this section has been adapted from the sample LDIF files on the Websphere Portal Installation Setup CD (PortalUsers.ldif and ContentUsers.ldif).

Create an LDIF file Containing Users

You must add the following user accounts to the directory:

- wpsadmin
- wpsbind

The absolute DN of these user accounts will be determined by the DIT structure of your directory. For this example, you will populate them into the following subtree:

```
c=au,o=democorp,ou=Administrators,ou=Websphere
```

To create the LDIF file containing users

1. Create the parent entries specified above.
2. In a text editor, create a new document.
3. Copy and paste the following LDIF representation into a new document:

```
dn: c=au
oc: top
oc: country
c: au

dn: o=democorp,c=au
oc: top
oc: organization
o: democorp

dn: ou=groups,o=democorp, c=au
oc: organizationalUnit
oc: top
ou: groups

dn: ou=users,o=democorp,c=au
objectClass: organizationalUnit
objectClass: top
ou: users

dn: uid=wpsadmin,ou=users,o=democorp,c=au
oc: inetOrgPerson
oc: organizationalPerson
oc: person
oc: top
userPassword: wpsadmin
uid: wpsadmin
cn: wps admin
sn: admin

dn: uid=wpsbind,ou=users,o=democorp,c=au
oc: inetOrgPerson
```

```
oc: organizationalPerson
oc: person
oc: top
userPassword: wpsbind
uid: wpsbind
cn: wps bind
sn: bind
```

4. Save the new file as *wpsusers.ldif*.

Create an LDIF file Containing Groups

You must add the following groups to the directory:

- wpsadmins
- wpsContentAdministrators
- wpsDocReviewer
- wcmadmins

To create the LDIF file containing groups

1. In a text editor, create a new document.
2. Copy and paste the following LDIF representation into a new document:

```
dn: cn=wpsContentAdministrators,ou=groups,o=democorp,c=au
objectClass: groupOfUniqueNames
objectClass: top
cn: wpsContentAdministrators
uniqueMember: uid=wpsadmin,ou=users,o=democorp,c=AU

dn: cn=wcmadmins,ou=groups,o=democorp,c=au
objectClass: groupOfUniqueNames
objectClass: top
cn: wcmadmins
uniqueMember: uid=wpsadmin,ou=users,o=democorp,c=AU

dn: cn=wpsDocReviewer,ou=groups,o=democorp,c=au
objectClass: groupOfUniqueNames
objectClass: top
cn: wpsDocReviewer
uniqueMember: uid=wpsadmin,ou=users,o=democorp,c=AU

dn: cn=wpsadmins,ou=groups,o=democorp,c=au
objectClass: groupOfUniqueNames
objectClass: top
cn: wpsadmins
uniqueMember: uid=wpsadmin,ou=users,o=democorp,c=AU
```

3. Save the new file as *wpsgroups.ldif*.

Load the LDIF Files Into the DSA

The DXmodify tool can load data from an LDIF file into a DSA.

To load the LDIF files

1. Use the following command to load the LDIF file containing the users:

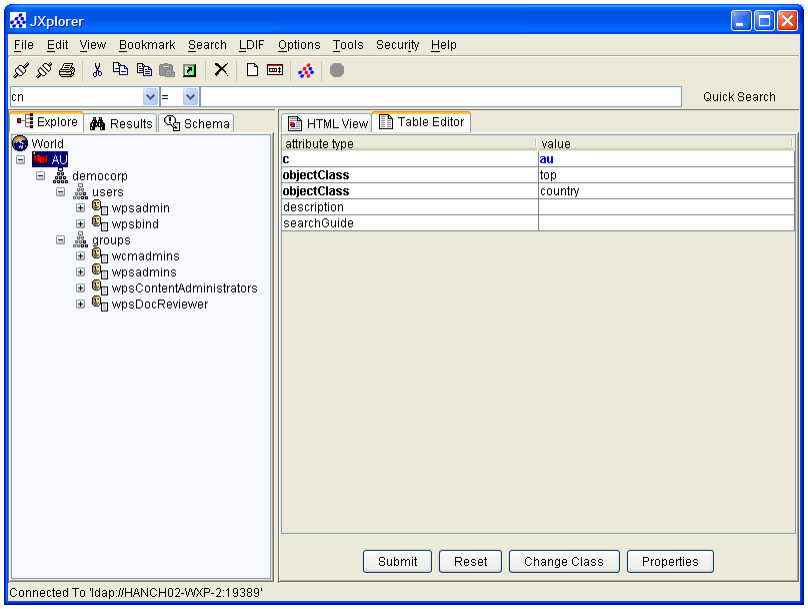
   ```
   dxmodify –a –c –h hostname –p 19389 –f wpsusers.ldif
   ```

2. Use the following command to load the LDIF file containing the groups:

   ```
   dxmodify –a –c –h hostname –p 19389 –f wpsgroups.ldif
   ```

3. When the load is completed, start JXwebplorer and connect to port 19389. User anonymous connection, as we have not activated any directory access controls as yet.

4. Once connected, expand all the DIT subtrees, and you should see exactly the same entries, as displayed in the image below.



You have now set up CA Directory act as the LDAP repository for Websphere Portal Server.

Set Up Websphere Portal Server

Now that you have set up the DSA containing the required data, you need to set up Websphere Portal Server.

The Websphere Portal Server installation uses about 4 GB of disk space. Ensure that you have adequate disk space before you install.

Install Websphere Portal Server

To install Websphere Portal Server

1. Log in as a user with administrator privileges.
2. Insert the Websphere Portal Server installation CD.

   If the installer does not start automatically, navigate to the CD drive and open the install.bat file.

   During the installation, the wizard will prompt you to supply information. The following table lists the information you need for each package:

Information	Recommendation
Select a language to be used for this wizard	Select your language
Software License Agreement	Read, and accept it if you agree.
Setup Type	Select *Full*
Websphere Application Server installation path	Confirm that this path is correct. Note: This full installation will consume approx 4 gigabytes of disk space. Ensure that you have adequate disk space before continuing.
Node name	Enter a name for this instance of WebSphere
WebSphere Application Server hostname	Enter the name of the computer that you are installing on
Websphere Portal installation directory	Confirm that this path is correct. **Note:** This full installation will consume approx 4 gigabytes of disk space. Ensure that you have adequate disk space before continuing.
System Logon User ID	If you want to start the Websphere components as a service, define a user account that the service can log in as.
WebSphere Portal administrative user	Create a user name and password that you will use later to log in to the Websphere portal. This user does not need to exist within Windows: this account is internal to the portal only.

3. Later in the installation process, enter the installation CDs when prompted.
4. In the last installation screen, de-select the Launch First Steps check box, and then click Finish.

   The installation has completed.
5. Restart the computer.

Configure Websphere Portal Server to Use CA Directory

Websphere Portal Server does not support CA Directory out-of-the-box. This means that you must configure Websphere Portal Server to think that CA Directory is Domino, one of the supported directories.

Edit the wpconfig.properties file

1. In a text editor, open the {wp_root}\config\wpconfig.properties file.

   This is the main Websphere Portal Server configuration file.

2. Edit the file to match the details shown below:

```
WasUserid=uid=wpsbind,ou=users,o=democorp,c=au
WasPassword=wpsbind
PortalAdminId=uid=wpsadmin,ou=users,o=democorp,c=au
PortalAdminIdShort=wpsadmin
PortalAdminPwd=wpsadmin
PortalAdminGroupId=cn=wpsadmins,ou=groups,o=democorp,c=au
WpsContentAdministrators=cn=wpsContentAdministrators,ou=groups,o=democorp,c=a
u
WpsContentAdministratorsShort=wpsContentAdministrators
WpsDocReviewer=cn=wpsDocReviewer,ou=groups,o=democorp,c=au
WpsDocReviewerShort=wpsDocReviewer
WcmAdminGroupId=cn=oucmadmins,ou=groups,o=democorp,c=au
WcmAdminGroupIdShort=Wcmadmins
LTPAPassword=password
LTPATimeout=120
LDAPHostName=hostname
LDAPPort=19389
LDAPAdminUId=uid=wpsadmin,ou=users,o=democorp,c=au
LDAPAdminPwd=wpsadmin
LDAPServerType=DOMINO502

LDAPBindID=uid=wpsbind,ou=users,o=democorp,c=au
LDAPBindPassword=wpsbind
LDAPSuffix=o=democorp,c=au
LDAPUserPrefix=uid
LDAPUserSuffix=ou=users
LDAPGroupPrefix=cn
LDAPGroupSuffix=ou=groups
LDAPUserObjectClass=inetOrgPerson
LDAPGroupObjectClass=groupOfUniqueNames
LDAPGroupMember=uniqueMember
LDAPUserFilter=(&(uid=%v)(objectclass=inetOrgPerson))
LDAPGroupFilter=(&(cn=%v)(objectclass=groupOfUniqueNames))
```

3. Save and close the configuration file.

Check that Required Entries Are Present

You must run the *validate-wmmur-ldap* script, which validates the contents of the *wpsconfig.properties* file with CA Directory. This confirms that all the required entries are stored within the directory.

To check that required entries are present

1. Run the following command from the {wp_root}\config folder:

```
WPSconfig.bat validate-wmmur-ldap –DWasPassword=wpsbind
-DPortalAdminPwd=wpsadmin –DLTPAPassword=password
–DLDAPAdminPassword=wpsadmin
–DWmmSystemIDPassword=wpsadmin
```

2. If the script finishes with the following, then the script ran to completion:

```
BUILD SUCCESSFUL
Total time: nn seconds
```

   If it failed, you should check the contents of the wpsconfig.properties file for a configuration error.

Switch the User Repository

You must run the *enable-security-wmmur-ldap* script, which switches Websphere's user repository from the default database to CA Directory.

This script will only work if the *validate-wmmur-ldap* script has run without error.

To switch to the CA Directory repository

1. Run the following command from the {wp_root}\config folder.

```
WPSconfig.bat enable-security-wmmur-ldap –DWasPassword=wpsbind
-DPortalAdminPwd=wpsadmin –DDbPassword=password
–DLTPAPassword=password
–DLDAPAdminPassword=wpsadmin
–DWmmSystemIDPassword=wpsadmin
```

2. If the script finishes with the following then the script ran to completion:

```
BUILD SUCCESSFUL
Total time: nn minutes nn seconds
```

Test the Integrated System

You have now finished integrating CA Directory with WebSphere Portal Server. The following sections describe how to test your system.

Log In to the Portal

You have switched Websphere Portal Security over to using CA Directory, so you should start your tests by logging in.

Log in to the portal

1. Open a browser and type in the following URL:

   `http://{FQDN of WPS server}:10038/wps/portal`

   The WebSphere Portal page opens.
2. Click the Log in link.
3. Log in using the following details:
   - User ID: wpsadmin
   - Password: wpsadmin
4. Click the Log in button.

   When the login process is complete, the portal view appears.
5. To log out, click the Log out button.

Create a New User In The Portal

The other way to test that the integration process is complete is to create a new user, and then log in as that user.

Create and log in as a new user

1. On the portal main page, click the Sign up button.
2. Type in the user's details, and then click OK to register the new user.

   When the user has been registered by the portal, the Congratulations screen appears.
3. Click Log in to to log in as the new user.
4. Type in the user ID and password, and then click Log in again.

   When the login has finished, the portal view appears.

   This will be different to the wpsadmin login you just performed, because the new user is not a member of the wpsadmins group within the directory.

Chapter 3: Integrate Entrust Security Manager

CA Directory is currently being certified with Entrust, using the *Entrust Ready Test Plan - Directories*.

This section contains the following topics:

Pre-requisites

Before you can integrate CA Directory and Entrust Security Manager, ensure that the following conditions are met:

- CA Directory is installed.
- The Informix patch (SM71P95992.zip) is available during the installation process.
- TCP/IP port 389 is not used by any other program.

  This section describes how to install Entrust using the simple integration, which automatically uses port 389.

Configure CA Directory

To integrate Entrust Security manager, you need to configure CA Directory by creating and configuring a DSA to store Entrust's internal policies and certificate-related data.

Create an Entrust DSA

You need to create a new DSA to store Entrust's internal policies and certificate-related data.

Use DXmanager to create a new backbone that includes a single DSA with the following details:

- DSA name: entrust
- TCP/IP connection port: 389
- DSA prefix: O=enTrust, C=AU

Configure the Entrust DSA

When you create a new DSA, the initialization file of the new DSA sources the default configuration files. In this case, the new Entrust DSA is set to use the default configuration files.

When you upgrade CA Directory, these default configuration files are overwritten, even if you have customized them.

To prevent an upgrade from overwriting the configuration files used by the Entrust DSA, you should create your own set of configuration files and set the Entrust DSA to use these.

To customize the Entrust DSA

1. Create copies of the following default configuration files:
   - Copy limits\dxmanager.dxc to limits\entrust.dxc
   - Copy logging\dxmanager.dxc to logging\entrust.dxc
   - Copy schema\dxmanager.dxg to schema\entrust.dxg (turn off the *read-only* flag)
   - Copy settings\dxmanager.dxc to settings\entrust.dxc
   - Copy database\dxmanager.dxc to database\entrust.dxc
2. Edit the *servers**entrust-Master-entrust.dxi* file to source the new configuration files.

   The DXI file should now look like this:

```
# Computer Associates DXserver
#
# Initialization file written by dxmanager
# logging and tracing
source "../logging/entrust.dxc";
# LEGACY licence
# source "../licence/dxmanager.dxc";
# schema
clear schema;
source "../schema/entrust.dxg";
# knowledge
clear dsas;
source "../knowledge/entrust.dxc";
# operational settings
source "../settings/entrust.dxc";
# service limits
source "../limits/entrust.dxc";
# database
source "../database/entrustdb.dxc";
# database settings
```

```
source "../database/entrust.dxc";
# access controls
clear access;
source "../access/dxmanager.dxc";
# replication agreements (rarely used)
# source "../replication/";
# multiwrite DISP recovery
set multi-write-disp-recovery = false;
# cache configuration
# set max-cache-size = 100;
# set cache-index = commonName, surname;
# set cache-attrs = all-attributes;
# set lookup-cache = true;
```

3. Open the schema file *schema/entrust.dxg* in a text editor.
4. Add the following line to the file:

   ```
   source "entrust.dxc";
   ```

5. Save and close the schema.
6. When the Entrust DSA is started, it will source the Entrust schema.
7. Confirm that the configuration files do not contain errors, using the following command:

   ```
   dxsyntax
   ```

   If no messages appear, the configuration contains no errors.

   If there are any errors, fix them, and then run *dxsyntax* command again.

Add Entries to the Entrust DSA

You need to create three entries in the Entrust DSA. These entries will store the Entrust data.

To add entries to the Entrust DSA

1. Start the DSA using the following command:

   ```
   dxserver start entrust
   ```

2. Create the following entries in the Entrust DSA.

   ```
   dn: ou=Certificates,o=enTrust,c=AU
   objectClass: organizationalUnit
   objectClass: enTrustCA
   objectClass: top
   ou: Certificates
   userPassword: {password}
   ```

   ```
   dn: ou=Admin,o=enTrust,c=AU
   objectClass: organizationalUnit
   objectClass: top
   ou: Admin
   dn: cn=DirAdmin,ou=Admin,o=enTrust,c=AU
   objectClass: inetOrgPerson
   objectClass: organizationalPerson
   objectClass: person
   objectClass: top
   cn: DirAdmin
   sn: DirAdmin
   userPassword: {password}
   ```

   The DSA's DIT should now show the following entries:

Install Entrust Security Manager

To install the Entrust Security Manager, you need to install the Informix Database, the Security Manager itself, and the Security Manager Administration.

Install the Informix Database

Before you can install Entrust Security Manager, you must install the patch for Informix 9.4 for Windows.

Follow the steps below to apply this patch, and then install the database software.

1. Download the full installation for Informix 9.4 for Security Manager 7.1.
2. Choose the "Unpack the files used to perform the installation to the location specified below, and don't remove these files after the setup is completed." option.
3. Run *Informix_9_4_for_easm_win.exe*.
4. Wait until the installation starts, and then cancel it.

   The files have been unpacked, and you can now find and run the patch.
5. Find the file SM71P95992.zip. This is the Informix patch.
6. Unzip the patch to a temporary directory.
7. Copy the patched version of *informix.msi* from the temp directory over the original version.
8. Continue with the installation, as described in the Entrust installation documentation.

   When the installation is finished, restart the computer as instructed.
9. Log in as the administrator.

   A post-installation script starts. When the script window closes, the installation process is complete.

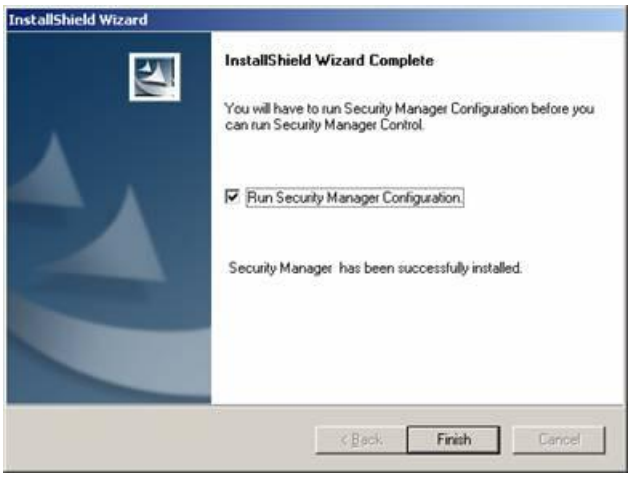
Install Entrust Security Manager

You should use the Entrust installation documentation to help you install Entrust Security Manager.

This section describes the only steps that will be defined here directly relate to the CA Directory configuration.

1. Install Entrust Security Manager.

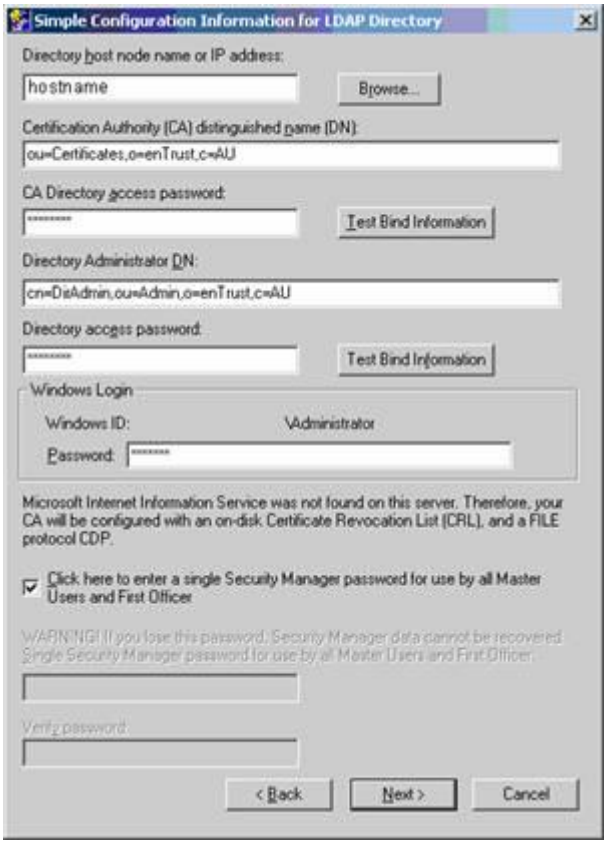
   After the installation process has been completed, the following screen will appear:



2. Select the *Run Security Manager Configuration* checkbox.
3. Click Finish.

   The Security Manager configuration wizard begins

4. Select the *Simple Configuration using LDAP Directory* from the dropdown list, and click Next.
5. Follow the standard installation process until the *Simple Configuration for LDAP Directory* dialog appears:



6. Add the Root CA certificate DN credentials, and click *Test Bind Information* to test these credentials.
7. Add the bind credentials of the administrative user, and click *Test Bind Information* to test these credentials.
8. Add the DSA connection information of the Entrust DSA that you created in Create an Entrust DSA (see page 36).

   The details should be entered as is displayed above. The only change may be in the DN structure, if you've created a different DN suffix to the “o=entrust,c=au” suffix used above.

   Note: You cannot use this dialog to change the TCP/IP port to connect to the DSA. This is set to port 389, which is the reason that you must set the Entrust DSA to use port 389.
9. Click Next, and continue to configure the Security Manager as described in the Entrust installation documentation.

Install Entrust Security Manager Administration

You must install Entrust Security Manager Administration. This lets CA Directory interface with Entrust Security Manager.

Install Entrust Security Manager Administration using the Entrust installation documentation.