hp knowledge brief

Provisioning to AD with HP OpenView Select Identity using LDAP over SSL

HP OpenView Select Identity can provision users and entitlements to Active Directory (AD) in two ways:

- Using the HP OpenView AD Agent, which runs as a Windows service and which needs to be installed on a Domain Controller or a Member Server
- Using the agent-less LDAP connector, which runs in the same application server as Select Identity and connects to AD over the internal network

Although the HP OpenView AD Agent is more powerful than the generic LDAP connector and provides features such as reverse notification and password synchronization, some customers prefer the non-intrusive approach of using a connector that connects to AD over the internal network.

In this case, the agent-less LDAP connector can be used. As the LDAP connector transfers sensitive information between AD and Select Identity, customers need to use LDAP over SSL (LDAPS).

Although the LDAP connector can be configured to use LDAPS simply by ticking a check box, there are some steps that need to be taken first in order to make sure that Select Identity (or the application server it is using) trusts the Certification Authority (CA) certificate that issued the SSL certificate.

This Knowledge Brief describes the steps required to implement LDAPS connectivity from Select Identity to an AD running on a Domain Controller. It should help others to avoid various pitfalls when configuring SSL connectivity.

In this example, BEA WebLogic 8.14 was used as the application server for Select Identity and the AD, running on Windows 2003.

Overview

The following steps are required for enabling SSL on the AD and configuring Select Identity using LDAP over SSL:

- Install Microsoft Certificate Services to enable SSL
- Export the Root CA Certificate from the AD
- Import the Root CA Certificate into BEA WebLogic certificate store
- Configure the Select Identity connector for LDAPS usage

Install Microsoft Certificate Services to enable SSL

In order to enable SSL connectivity to the AD, Microsoft Certificate Services need to be installed within the Domain. After configuring an Enterprise Root CA and rebooting the system, the Root CA automatically creates an SSL certificate for AD and thus enables LDAPS connections to the AD.

For more details about installing and testing Microsoft Certificate Services see [3].

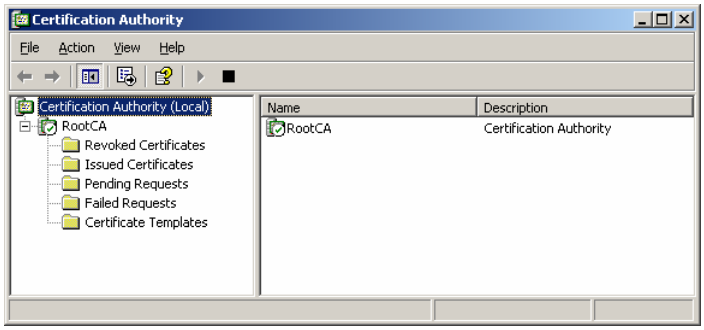
Verifying CA Installation

After the installation, the AD system needs to be rebooted. LDAPS should now be enabled on the AD. This can be verified by pointing Internet Explorer to https://<ip address of ad>:636 (the LDAPS port of AD). Internet Explorer should display a security alert similar to the following:

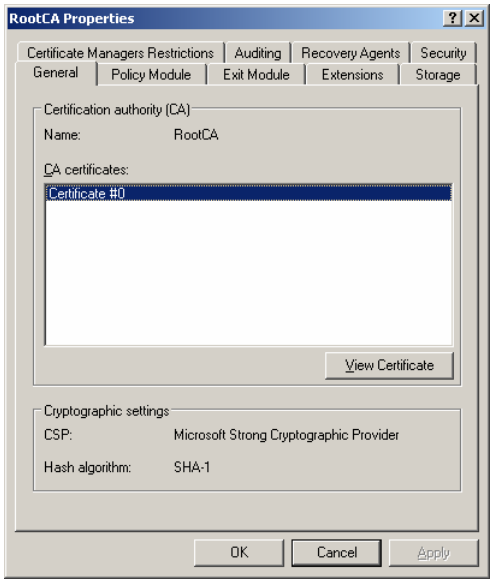
See [3] for further ways of testing the connectivity.

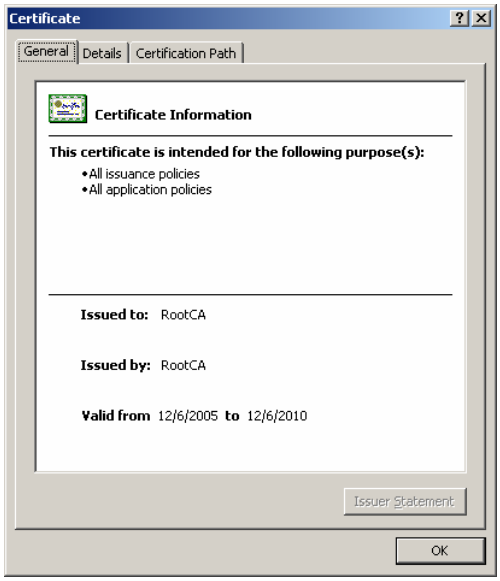
Export Root CA Certificate from AD

1. The Root CA certificate can be exported by launching *Start -> Administrative Tools -> Certification Authority* on the Domain Controller. Right click on *RootCA* and select *Properties*.



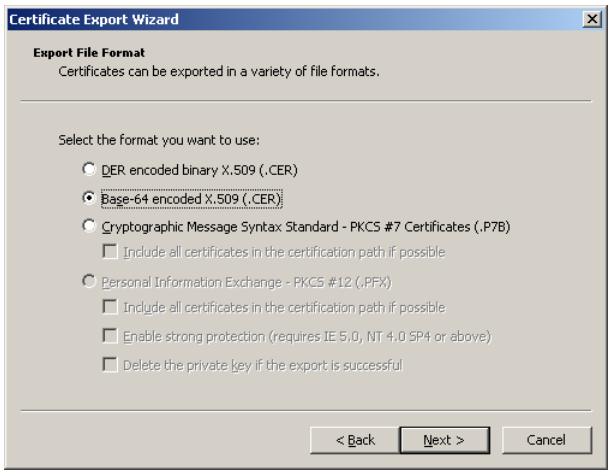
2. Click on *View Certificate*. In the certificate dialog box, select the *Details* tab and select *Copy to File*.



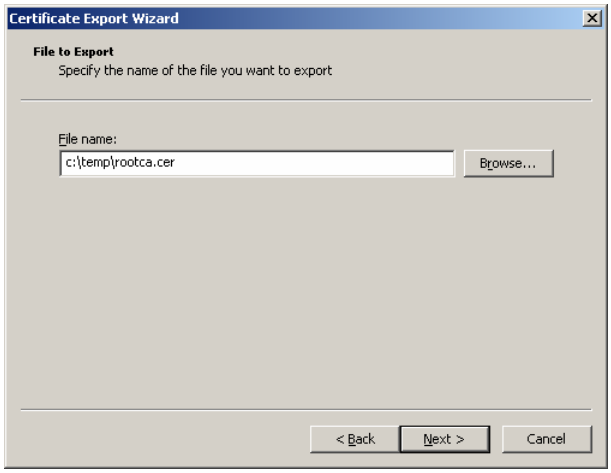


3. Click on *Next*.

4. Select *Base-64 encoded X.509 (.CER)*



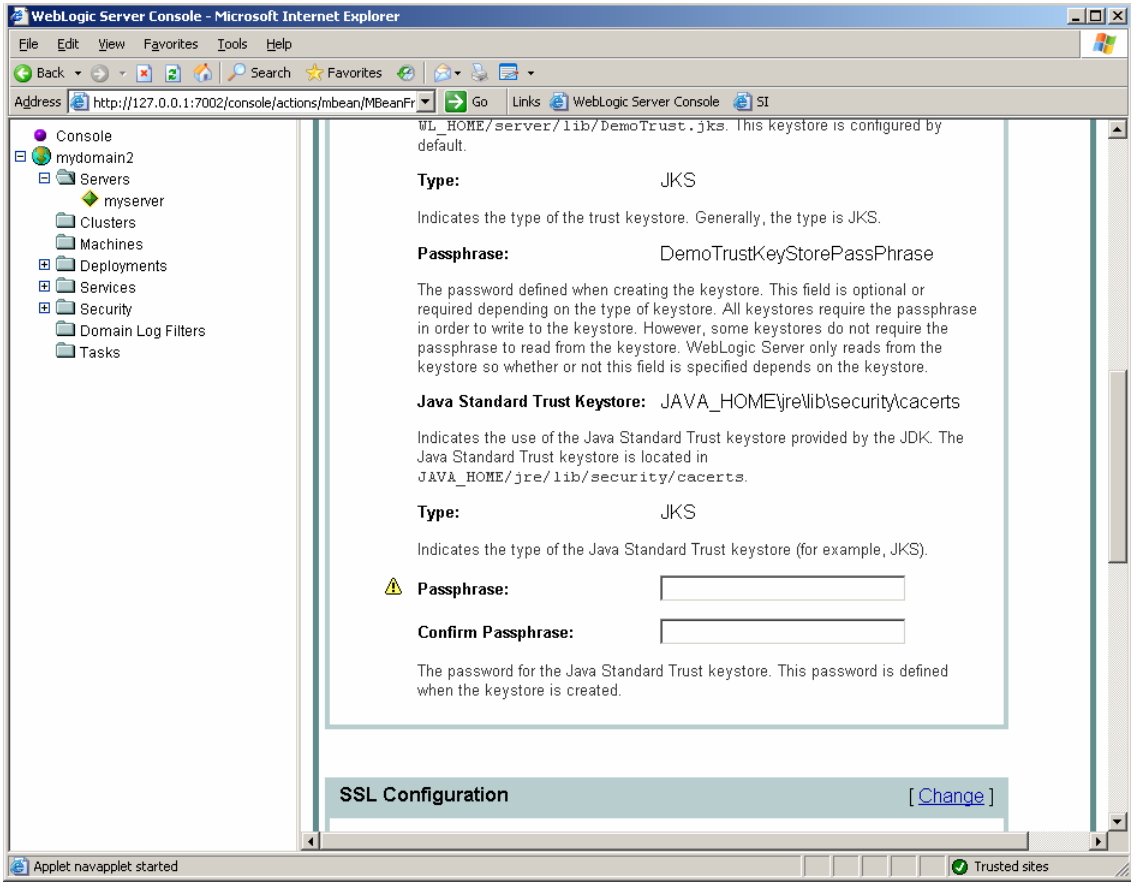
5. Enter the filename for the certificate.



6. Select *Finish* to export the certificate.

Import the Root CA Certificate into the BEA WebLogic certificate store

1. By default, BEA WebLogic (and therefore Select Identity) uses the <WL_HOME>/jdk_142_05/jre/lib/security/cacerts as the Java Standard Trust keystore. This contains all trusted Root CA certificates. This can be verified in the BEA WebLogic console by looking at the *KeyStores & SSL* tab.



2. The standard Java keytool utility can be used to import the Root CA certificate into the Java Standard Trust keystore:

```
keytool -import -v -file c:\temp\rootca.cer -keystore cacerts
-storepass changeit
```

Please note that the default password for the keystore *cacerts* is *changeit*.

3. Output similar to the following should be shown:

```
Owner: CN=RootCA, DC=bbn, DC=hp, DC=com

Issuer: CN=RootCA, DC=bbn, DC=hp, DC=com

Serial number: 1cb49c24ec18ce9c4f38165fb2418dca

Valid from: Tue Dec 06 15:37:14 CET 2005 until: Mon Dec 06 15:46:17 CET 2010

Certificate fingerprints:

        MD5:  45:7A:18:5E:4E:B7:F9:53:53:EE:EC:71:85:EE:9F:90
```

```
        SHA1: 75:F5:33:0C:98:11:CF:5B:C3:B9:A9:BA:7A:C0:84:72:54:40:8B:E1

Trust this certificate? [no]:  yes

Certificate was added to keystore

[Storing cacerts]
```

4. The following command can be used to verify if the certificate has really been added to the keystore:

```
keytool -list -v -keystore cacerts -storepass changeit | more
```

Note: A separate trust store can be used as an alternative to using the BEA default certificate trust store. A separate trust store can be used by adding the following BEA WebLogic startup parameters:

```
-Djavax.net.ssl.trustStore=/opt/bea/jdk142_05/jre/lib/security/cacerts
-Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.debug=ssl,handshake,data,trustmanager
```

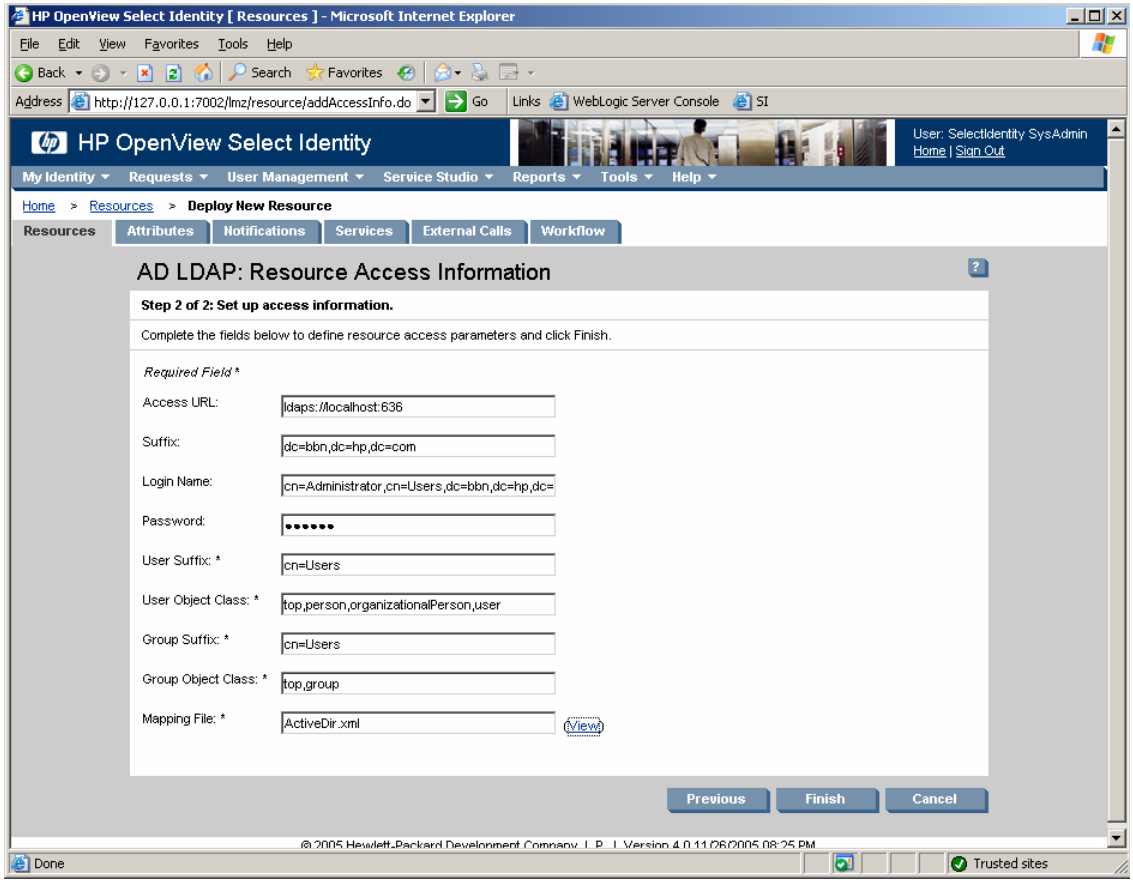
---

5. If SSL connectivity to the AD needs to be verified using another Java application (e.g. LDAP Browser, http://www-unix.mcs.anl.gov/~gawor/ldap), the Root CA certificate needs to be imported into the default keystore used by the Java applications. By default, Java is uses the *.keystore* file in the user's home directory. The following command imports the Root CA certificate into this keystore:

```
keytool -import -v -file c:\temp\rootca.cer -storepass <mypassword>
```

Configure the Select Identity connector for LDAPS usage

The following screen shot shows the parameters that need to be configured to connect to the AD using LDAPS:



After pressing the Finish button, Select Identity connects to the AD using LDAPS and reports a successful connection. Following this the resource can be used within Select Identity and further configuration steps can be performed (for example, Attribute Mapping, Recon policies, service assignment etc.).

References

[1] Details about the Java keytool can be found at:
http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html

[2] Windows Certificate Services “How To”:
http://technet2.microsoft.com/WindowsServer/en/Library/4755cb22-57f3-4d3f-a0d1-d2385743d2201033.mspx

[3] KB2648, Leveraging SSL for Secure LDAP Communications,
http://cgscomm3.inet.cpqcorp.net/Technology/Documents/Knowledge%20Briefs/Q1FY06/KB2648.doc