

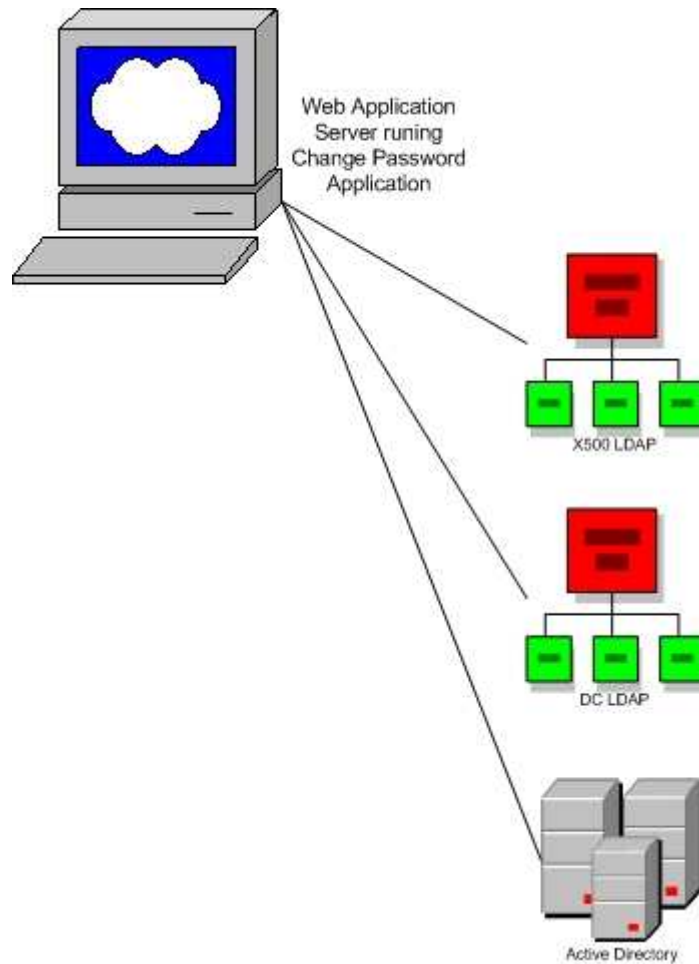
White Paper: Password Synchronization between aeSLAPD and Active Directory

Scope: Provide information required to synchronize the aeSLAPD password into MS Active Directory. Password changes will occur against a single LDAP authenticated JSP which will provide password policy checking, a list of policy compliant randomly generated passwords for user's discretionary use. If at any time an error should occur in the process, an error message will be displayed telling the user where the failure occurred.

The program is designed to maintain synchronization of user passwords between AESLAPD and MS AD and possibly other LDAP enabled directories. Specific criteria with regard to MS AD password synchronization occurs that is non germane to other LDAP directories and special attention is required. Connection to AD for password changes REQUIRES an SSL connection and the certificate format REQUIRED by MS is specific in terms of the cert profile. MS AD will NOT allow just any valid identity certificate to work for SSL and password changes. Also, the ldif information for the password requires special specific ASN.1 encoding prior to submission to AD. This application makes connections to multiple directories in sequence and attempts to change the password for the identified user in each directory. Primary authN occurs at the Enterprise aeLAPD directory via LDAP uid/password or the user's x509 UT certificate, then privileged connections are made to the directories to make the change. If a particular directory is not accessible an error for that connection is reported to the user but other connection will complete successfully unless otherwise noted. The application provides logic to force the user to provide a password that complies with UT Password Policy. The application is a JSP over https and is and will time-out after 5 minutes of user inactivity.

Program Flow

1. User connects to JSP
2. User is authenticated to aeSLAPD via uid/password or UT Issued X509 user certificate
3. Application screen is re-painted with password logic screen requesting user to change their password according to the displayed password policy. A list of randomly generated compliant passwords is generated for the user to use at their discretion.
4. An SSL connection is made to oac15 (X500 LDAP)
5. Password is changed on oac15 first and if successful proceed else throw an error telling which connection failed
6. An SSL connection is made to oac7 (DC LDAP)
7. Password is changed on oac7 and if successful proceed else throw an error telling which connection failed
8. An SSL connection is made to UTHSCH AD
9. Password is changed on UTHSCH AD (clear text password is Unicode encoded using a special Unicode class)
10. If successful a success message is returned to the user's browser



NOTE**: General Cert Profile information:

1. Recommend using AD CA services as the default will issue the correct profile IF, the CA service issues an SSL cert from the Enterprise Root CA. You must install the service under the ROOT as Enterprise Domain Admin. This is the only way to get the CRL imbedded which is required to make an SSL connection.
2. When issuing the certs, make certain that the date will span your needs for a while.
3. Issue multiple certs just in case and keep a spares available to the applications.
4. Since these are issued out of a private root, they will need to be trusted / installed in the application root store.
5. If it does not work with LDP and not logged into the domain, you have not done it right.
6. Logging into the domain implies a trust that is different from an SSL/TLS connection always test outside of the domain.

Installing CA services in Microsoft AD

In order to change the password in MS AD, an SSL connection is required using a certificate who's profile is compliant with MS requirements in a number of areas.

Install Certificate services on the server.

1. Prior to running the Cert services installation wizard, Service pack 3 must be installed/re-installed. You will also need to download critical update Q323172 for Windows 2000. This update resolves the "Flaw in Digital Certificate Enrollment Component Allows Certificate Deletion" security vulnerability in Windows 2000. Install the update in step 13.
2. Start>settings>control panel
3. Add remove programs
4. Add/remove Windows Components
5. Check Certificate Services. You will get a pop-up menu telling you that the computer cannot be renamed and that the computer cannot join or be removed from a domain. Click Yes to proceed.
6. The Windows component wizard will prompt you to select the terminal services mode. Select Remote Administration Mode. Click next.
7. On the Certification Authority Type Selection Page, select the type of Certificate server you want (Enterprise root, Enterprise subordinate, etc.). In order to store a copy of the certificate revocation list in Active Directory, choose Enterprise CA. In a root (parent) domain, select Enterprise root CA. For a child domain, select Enterprise subordinate CA.
8. Select Advanced Options. Click next
9. On the Public and Private key Selection Page, for the Cryptographic Service provider, select Microsoft Enhanced Cryptographic Provider ver. 1.0. Select the key length (the default is 512 bits, 2048 or greater is recommended)
10. Use the default hash algorithm (SHA-1), key length, etc. Click next
11. On the CA identifying information page, enter the fully qualified domain name for the CA. Enter information for the Organization, OU, locality, State, email address and CA description. Click next.
12. On the Data Storage Location Page, take the default storage location for the certificate database and logs. On the Store configuration in a shared folder name, click browse and navigate to the Trusted Root Certificate Store and install the certificate to that location. Click next to finish.
13. Install Critical update Q323172 and reboot the computer.
14. At this point, Certificate Services is installed with a CA certificate. By default, on an Enterprise CA, certificates are automatically issued upon request. A server authentication cert should be automatically generated.
15. Next, confirm the installation. Start>run>mmc. On the Console menu, click add/remove snap-in.>Certificates>computer account>local computer>finish.
16. Open the Personal folder and the certificates folder. Confirm that there are two certificates. One certificate will have Client authentication for its intended purpose and the other certificate will have all for its intended purpose.
17. Double click the Client Authentication cert and click the Certification path. It should be chained under the CA cert.
18. Confirm that you can make an SSL connection to the server from the server. Install the support tools on the server from the Windows 2000 CD. Run LDP Start>Programs>Windows 2000 support tools>tools>Active Directory Administration Tool. On the LDP menu bar select connection>connect. In the server window type the fully qualified domain name of the CA. In the port window, enter 636. Leave the connectionless window unchecked. Click ok. You should get an LDAP open message that shows you have connected to the CA. On the menu bar, click connection>bind. Enter a user account, password and domain in the domain. You will get a message that states authenticated as user %username%. On the menu bar, click view>tree. Leave the BaseDN blank and click ok. In the left pane, you should see the OU structure in Active Directory.
19. Download the CA cert to a client machine and repeat SSL connection to AD with the LDP support tools described in step 18. To download the CA cert on a client, open Internet Explorer and enter the URL **Error! Bookmark not defined.** Click retrieve the CA certificate or certificate revocation list and click next. Click Install this CA certification path. After the cert is downloaded you should be able to open LDP on the client, connect to the CA over port 636, bind to the directory with a domain admin account and view the AD tree as described in step 18.

To Uninstall Certificate Services from a domain controller:

1. Remove the Certificate Services component from the server. Start>Settings>Control Panel>Add Remove programs>Add Remove Windows Components. Uncheck Certificate Services.
2. Reboot the server into Directory Services restore mode. Delete the Certlog and Certsrv folders from Winnt/system32 folder. Reboot the server.
3. Open Regedit and remove the certsrv folder from the registry
HKEY_Local_Machine\System\CurrentContolSet\Services\
HKEY_Local_Machine\System\CurrentContolSet\Services\
4. Open ADSIedit from the support tools and remove the following: Configuration>CN=Services,CN=Public Key Services,CN=AIA (delete the AIA folder). CN=CDP (delete the folders under CDP), CN=Certification Authorities (delete folder), CN=Enrollment Services (delete folder)

Application Specifics

- Location: /var/JAVA/src/jsp/auth
- Run via web access from user or authorized administrator
- Javadocs available