ACTIVE DIRECTORY WITH SSL

Active Directory with SSL

Active Directory LDAP SSL

How to Enable Active Directory LDAP SSL

Installing an Enterprise Root Certificate Authority in Windows Server 2008/2012/2016.

In order to install and configure an Enterprise Root CA, you must log onto the server with a user account that belongs to the Domain Admins group.

1. To Set Up an Enterprise Root CA in Windows Server 2008/2012/2016

1. Click Start, point to Administrative Tools and then click Server Manager.
2. In the Roles Summary section, click Add Roles.
3. On the Select Server Roles page, select the Active Directory Certificate Services check box.

Click `Next` two times.

4. On the Select Role Services page, select the Certification Authority check box, and then click `Next`.
5. On the Specify Setup Type page, click Enterprise, and then click `Next`.
6. On the Specify CA Type page, click Root CA, and then click `Next`.
7. On the Set Up Private Key and Configure Cryptography for CA pages, you can configure optional configuration settings, including cryptographic service providers.

Click `Next` twice.

8. In the Common name for this CA box, type the common name of the CA. The common name for a CA is usually the same as its hostname or computer name. Keep in mind as well, that you will not be able to change any of the identifying information after the service is installed.
9. Click `Next`.
10. On the Set the Certificate Validity Period page, configure the default validity duration for the root CA. The Validity period defines how long issued certificates remain valid. The default value for this field is 5 years. You can increase or decrease the number as necessary. Click `Next` after you have filled in the information.
11. On the Configure Certificate Database page, configure the location of the Certificate database, the Certificate database log, and the shared folder. The default location for the database and database log is `C:\WINDOWS\system32\CertLog`. You use the default value or use the Browse button to select a different location. Click `Next`.
12. After verifying the information on the Confirm Installation Options page, click `Install`.

Setup will configure the necessary components. If setup cannot locate the necessary files, you will be prompted for the Windows Server 2008 CD-ROM to continue. If IIS is not installed, a warning will appear. IIS is required in order to use Certificate Services

Web Enrollment Support. Click `OK` to acknowledge the message.

Review the information on the confirmation screen to verify that the installation was successful.

2. Downloading and configuring the AD CA certificate into WebADM

Once the Active Directory domain controller is configured, you can download the CA certificate and configure it into the WebADM server. This will enforce server certificate validation on the LDAP connection.

To download the AD CA certificate you can use the included OpenSSL on the WebADM server. Please note that you must change the following input with your own AD DC IP and port into the command:

```
echo -n | /opt/webadm/libexec/openssl s_client -connect <AD_SERVER_IP>:636  | \
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /opt/webadm/conf/ad.crt
```

Now you should have the CA certificate in `/opt/webadm/conf/ad.crt` which can be configured into the `servers.xml` or your LDAP mount point configuration in WebADM.

In `servers.xml`:

```
<LdapServer name="AD DC"
 host="<AD_SERVER_IP>"
 port="636"
 encryption="SSL"
 ca_file="/opt/webadm/conf/ad.crt"
 cert_file="/opt/webadm/conf/ad_cert.cer"
 key_file="/opt/webadm/conf/ad_key.cer"

 />
```

`cert_file` and `key_file` are optional, in case the LDAP server requires a client certificate. For example, Azure AD can be reached with LDAP but ONLY if you have client certificate (PEM format).

For a mountpoint, configure the cert file in WebADM > Admin > LDAP Mount Points > CONFIGURE > Trusted CA certificate.