How to enable LDAP over SSL with a third-party certification authority

This article was previously published under Q321051

Article ID : 321051
Last Review : August 3, 2005
Revision : 9.0

SUMMARY

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to Active Directory. By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology. You can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate from either a Microsoft certification authority (CA) or a non-Microsoft CA according to the guidelines in this article.

MORE INFORMATION

There is no user interface for configuring LDAPS. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic.

Requirements for an LDAPS certificate

To enable LDAPS, you must install a certificate that meets the following requirements:

- The LDAPS certificate is located in the Local Computer's Personal certificate store (programmatically known as the computer's MY certificate store).
- A private key that matches the certificate is present in the Local Computer's store and is correctly associated with the certificate. The private key must *not* have strong private key protection enabled.
- The Enhanced Key Usage extension includes the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
- The Active Directory fully qualified domain name of the domain controller (for example, DC01.DOMAIN.COM) must appear in one of the following places:
  - The Common Name (CN) in the Subject field.
  - DNS entry in the Subject Alternative Name extension.
- The certificate was issued by a CA that the domain controller and the LDAPS clients trust. Trust is established by configuring the clients and the server to trust the root CA to which the issuing CA chains.

For more information about establishing trust for certificates, see the "Policies to establish trust of root certification authorities" topic in Windows 2000 Server Help.

Creating the certificate request

Any utility or application that creates a valid PKCS #10 request can be used to form the SSL certificate request. Use Certreq to form the request.

Certreq.exe requires a text instruction file to generate an appropriate X.509 certificate request for a domain controller. You can create this file by using your preferred ASCII text editor. Save the file as an .inf file to any folder on your hard drive.

To request a Server Authentication certificate that is suitable for LDAPS, follow these steps:

1. Create the .inf file.

   Following is a example .inf file that can be used to create the certificate request:

```
----------------- request.inf -----------------
[Version] Signature="$Windows NT$
[NewRequest] Subject = "CN=<DC fqdn>"
; replace with the FQDN of the DC KeySpec = 1 KeyLength = 1024
; Can be 1024, 2048, 4096, 8192, or 16384.
; Larger key sizes are more secure, but have
; a greater impact on performance.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
```

```
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0 [EnhancedKeyUsageExtension] OID=1.3.6.1.5.5.7.3.1

; this is for Server Authentication
-----------------------------------------------
```

Cut and paste the sample file into a new text file named Request.inf. Provide the fully qualified DNS name of the domain controller in the request.

2. Create the request file. To do this, type the following command at the command prompt, and then press ENTER:

   certreq -new request.inf request.req

   A new file called Request.req is created. This is the base64-encoded request file.

3. Submit the request to a CA. You can submit the request to a Microsoft CA or to a third-party CA.
4. Retrieve the certificate that is issued, and then save the certificate as Certnew.cer in the same folder as the request file. To do this, follow these steps:
   a. Create a new file called Certnew.cer.
   b. Open the file in Notepad, paste the encoded certificate into the file, and then save the file.

   Note The saved certificate must be encoded as base64. Some third-party CAs return the issued certificate to the requestor as base64-encoded text in an e-mail message.
5. Accept the issued certificate. To do this, type the following command at the command prompt, and then press ENTER:

   certreq -accept certnew.cer

6. Verify that the certificate is installed in the computer's Personal store. To do this, follow these steps:
   a. Start Microsoft Management Console (MMC).
   b. Add the Certificates snap-in that manages certificates on the local computer.
   c. Expand **Certificates (Local Computer)**, expand **Personal**, and then expand **Certificates**.

   A new certificate should exist in the Personal store. In the **Certificate Properties** dialog box, the intended purpose displayed is **Server Authentication**. This certificate is issued to the computer's fully qualified host name.
7. Restart the domain controller.

A private key that matches the certificate is present in the Local Computer's store and is correctly associated with the certificate. The private key must not have strong private key protection enabled.

To access the Local Computer's store, start the Certificates snap-in. At the prompt, click **Computer Account**, and then click **Local Computer**. Click **Personal**, and then right-click **Certificates**. Click **All Tasks/Request New Certificate**. Go through the wizard to request a domain controller certificate.

For more information about creating the certificate request, see the following Advanced Certificate Enrollment and Management white paper:

Verifying an LDAPS connection

After a certificate is installed, follow these steps to verify that LDAPS is enabled:

1. Start the Active Directory Administration Tool (Ldp.exe).

   This program is installed in the Windows 2000 Support Tools.
2. On the **Connection** menu, click **Connect**.
3. Type the name of the domain controller to which you want to connect.
4. Type **636** as the port number.
5. Click **OK**.

RootDSE information should print in the right pane, indicating a successful connection.

Possible issues

- **Start TLS extended request**
  LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged. Windows 2000 does not support the Start TLS extended-request functionality.
- **Multiple SSL certificates**
  Schannel, the Microsoft SSL provider, selects the first valid certificate that it finds in the local computer store. If there are multiple valid certificates available in the local computer store, Schannel may not select the correct certificate.
- **Pre-SP3 SSL certificate caching issue**
  If an existing LDAPS certificate is replaced with another certificate, either through a renewal process or because the issuing CA has changed, the server must be restarted for Schannel to use the new certificate. The SSL provider in Windows 2000 caches the LDAPS certificate and does not detect the change until the domain controller is restarted. This has been corrected in Service Pack 3 for Windows 2000.

APPLIES TO

- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Advanced Server

Keywords: kbinfo KB321051