

ITPro™
SERIES

WindowsITPro eBooks

By Jan De Clercq

Understanding and Leveraging

SSL-TLS for Secure Communications



Contents

Chapter 4: Leveraging SSL for Secure LDAP, SMTP, and NNTP	62
Leveraging SSL for Secure LDAP	62
Microsoft AD LDAP over SSL Support	63
Setting Up LDAP over SSL for AD	63
Windows DC LDAPS Certificate Enrollment	65
Testing LDAP over SSL for AD	67
Leveraging SSL for Secure SMTP	71
Setting up SMTP over SSL for Exchange Server 2003	71
Configuring SMTP over SSL for Exchange Server 2003	74
Testing SMTP over SSL for Exchange Server 2003	77
Leveraging SSL for Secure NNTP	79
Conclusion	82

Chapter 4:

Leveraging SSL for Secure LDAP, SMTP, and NNTP

This chapter focuses on how you can leverage Secure Sockets Layer/Transport Layer Security (SSL/TLS) for secure Lightweight Directory Access Protocol (LDAP), SMTP, and Network News Transfer Protocol (NNTP) communications. The three scenarios are illustrated in a Windows Active Directory (AD) environment for secure LDAP, and in the Microsoft Exchange Server 2003 mail-server environment for secure SMTP and NNTP.

Remember from the previous chapters of this eBook that you can use SSL to provide authentication, content-confidentiality, and integrity-protection services for application-layer protocols (including LDAP, SMTP, and NNTP). SSL does not, however, provide end-to-end data protection; it secures the data only while it is being transmitted over the SSL channel.

Leveraging SSL for Secure LDAP

The LDAP has become the de facto standard for accessing and interacting with directories. The LDAP defines a standard communications format for querying the data stored in X.500-formatted directories. All commercial (e.g., Microsoft AD, Novell eDirectory) and noncommercial (e.g., openLDAP) directory products available today support LDAP.

The latest LDAP version, Lightweight Directory Access Protocol version 3 (LDAPv3), is defined in Requests for Comments (RFCs) 2251 through RFC 2256—RFC 2251, “Lightweight Directory Access Protocol (v3)”; RFC 2252, “Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions”; RFC 2253, “Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names”; RFC 2254, “The String Representation of LDAP Search Filters”; RFC 2255, “The LDAP URL Format”; and RFC 2256, “A Summary of the X.500(96) User Schema for Use with LDAPv3”). You can access all these and other LDAP-related RFCs mentioned in this chapter from <http://www.ietf.org/rfc>, the Internet Engineering Task Force (IETF) URL.

The initial LDAP specifications do not provide security services such as user authentication and access control, or confidentiality and integrity protection for the data transmitted between an LDAP client and server. LDAP authentication methods were added in RFC 2829, “Authentication Methods for LDAP.”

For content security (confidentiality and integrity protection), LDAP builds on protocols such as SSL/TLS. This means that if you don't set up SSL/TLS protection, by default, all data transmitted between an LDAP client and server is transmitted in the clear. A set of TLS-specific functions for LDAP was added in RFC 2830, “Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.”

LDAP over SSL is also referred to as LDAPS. By default, LDAPS uses TCP port 636. Standard LDAP uses TCP port 389. You must know these port numbers if you want to connect to an LDAP- or LDAPS-enabled directory.

In addition to the dedicated port number for LDAPS (TCP/636), most LDAPS implementations also support another method for setting up the LDAPS connection, which is to use the StartTLS and StopTLS commands. You can use these commands to switch the LDAP connection to LDAPS after you connect to the LDAP server over the standard LDAP port (TCP/389).

Microsoft AD LDAP over SSL Support

AD is Microsoft's LDAP-accessible directory that comes bundled with the Microsoft Windows 2000 and Windows Server 2003 server OSs. In the Windows Server 2003 R2 release (at the time of this writing, the release is planned sometime in early 2006), Microsoft includes a standalone version of AD called Active Directory Application Mode, or ADAM. ADAM is also available as a separate download for Windows 2000 and Windows Server 2003. ADAM is a lightweight AD that lets enterprises easily deploy an LDAP-accessible directory for their applications—without having to bother about AD's domain and security-infrastructure features. You can find more information about AD at <http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx> and about ADAM at <http://www.microsoft.com/windowsserver2003/adam/default.mspx>.

In the following sections, we explain how you can configure and test LDAP over SSL support for AD. With this configuration, all LDAP traffic between AD or ADAM and an LDAP client will be protected in terms of both confidentiality and integrity. You also can apply to ADAM the instructions outlined in the section “Setting up LDAP over SSL for AD”.

Table 4-1 summarizes the default LDAP and LDAPS ports as they are used by Windows and Windows Server 2003 (both AD and ADAM). Note that AD supports an additional set of LDAP and LDAPS ports for domain controllers (DCs) that are also Global Catalog (GC) servers. GC servers are special-purpose DCs that contain a subset of the data defined in all domains of a Windows AD forest.

Table 4-1 Windows AD LDAP-related ports

Function/Protocol	Port Number
Domain Controller/LDAP	TCP/389
Domain Controller/LDAP over SSL (LDAPS)	TCP/636
Global Catalog DC/LDAP	TCP/3268
Global Catalog DC/LDAP over SSL (LDAPS)	TCP/3269

Windows 2000 and Windows Server 2003, however, currently do not support the StartTLS and StopTLS commands for setting up LDAPS connections to AD or ADAM.

Setting Up LDAP over SSL for AD

LDAP over SSL always requires a server-side LDAPS certificate. When you are configuring LDAPS for securing LDAP access to AD, an LDAPS certificate must be linked to the Windows DC server.

The LDAPS certificate linked to the Windows DC server must have the following characteristics:

- The LDAPS certificate must be stored in the Local Computer Personal Certificates store of the AD domain controller. Programmatically, this store is also referred to as the computer's My Certificate store.

You can access a Windows machine's Local Computer Personal Certificates store from the Microsoft Management Console (MMC) Certificates snap-in. To do so, you must load the

Local Computer account's certificate store (as Figure 4-1 illustrates), and then open the Personal Certificates store container (as Figure 4-2 illustrates).

Figure 4-1

Loading a Windows computer account's Certificate store

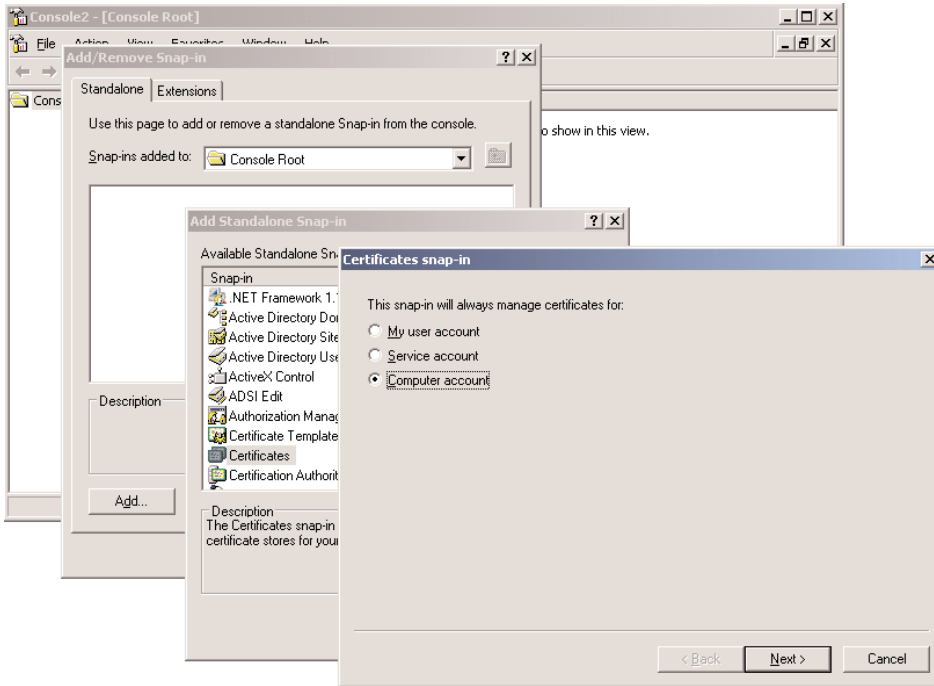
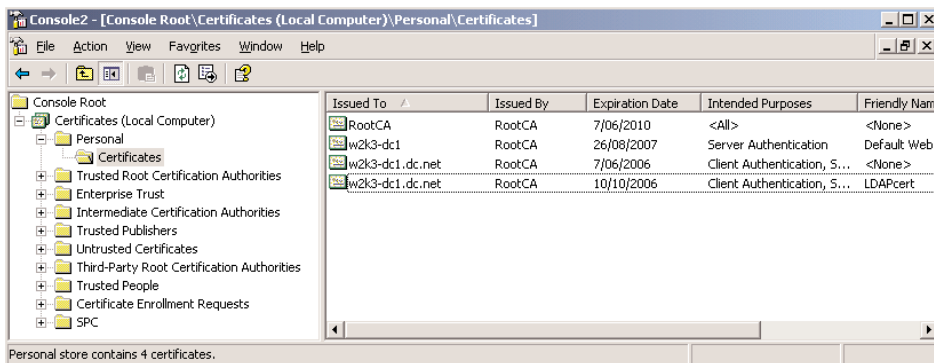


Figure 4-2

Opening the Personal Certificates store in the MMC Certificates snap-in



- The private key associated with the LDAPS certificate must be stored in the Local Computer's private key store.
- The private key associated with the LDAPS certificate must not have strong private-key protection enabled. Strong private-key protection is an advanced Windows private-key protection mechanism that uses a password to secure the access to a private key; the mechanism prompts for this password each time the private key is accessed.
- The Enhanced Key Usage extension of the LDAPS certificate must include the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (OID).
- The Fully Qualified Domain Name (FQDN) of the DC must appear in one of the following X.509 certificate fields of the LDAPS certificate:
 - The common name (CN) in the Subject X.509 field.
 - The DNS entry in the Subject Alternative Name X.509 extension.
- The LDAPS certificate must be issued by a Certification Authority (CA) that the DC and LDAP clients trust. CA trust can be established by configuring the clients and the server to trust the root CA to which the issuing CA chains. We explained certificate trust in greater detail in chapter 3 of this eBook.

Windows DC LDAPS Certificate Enrollment (3)

Windows supports different mechanisms to enroll a Windows DC for an LDAPS certificate:

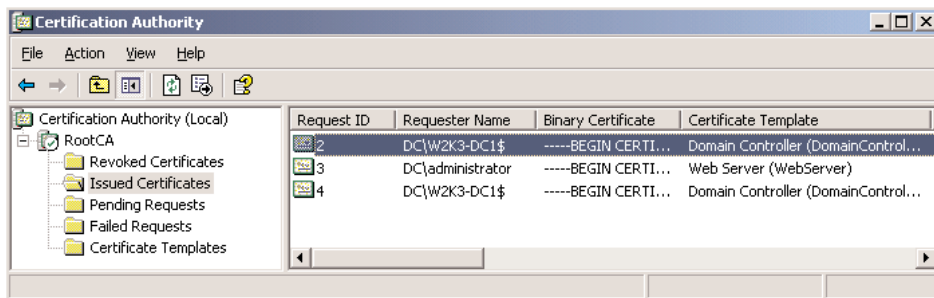
- Machine certificate autoenrollment
- Manual enrollment using the Certificate Request Wizard
- Manual enrollment using the certreq.exe command-line utility

Machine certificate autoenrollment and manual enrollment using the Certificate Request Wizard are available only in Windows 2000 or Windows Server 2003 AD forests that have Windows enterprise CAs installed. A Windows enterprise CA is an AD-integrated CA.

When you install an Enterprise CA, all DCs in the forest will automatically request a certificate to support LDAPS using SSL port 636. You can view the automatic issuance of the LDAPS certificate for DCs from the MMC Certificate Authority snap-in of the enterprise CA (as Figure 4-3 illustrates). This autoenrollment feature also applies to the renewal of DC LDAPS certificates that are about to expire.

Figure 4-3

Observing machine certificate autoenrollment behavior for LDAPS DC certificates



Administrators also can enroll DC servers manually for LDAPS certificates. To enroll for LDAPS certificates using the Certificate Request Wizard, start the MMC Certificates snap-in, and load the Local Computer certificate store (explained in the previous section). In the Wizard, select either the Domain Controller or Domain Controller Authentication certificate type (both types include the server authentication-enhanced key usage that links to OID 1.3.6.1.5.5.7.3.1, which is required for LDAPS authentication). This scenario is very similar to autoenrollment: After the LDAPS certificate request has been sent, the CA will generate the certificate, and the certificate automatically will be installed in the Local Computer's certificate store. This enrollment method is available only if you have a Windows enterprise CA installed in your environment.

In environments that do not have a Windows enterprise CA installed (but have instead, for example, a Windows standalone, or non-AD-integrated, CA), or when you must request the LDAPS certificate from a commercial CA such as Thawte or Verisign, you can use the `certreq.exe` command-line utility to get your server's LDAPS certificate. To obtain an LDAPS certificate using `certreq.exe`, use the following steps:

1. Create an `.inf` configuration file to generate the LDAPS certificate request. This configuration file must be formatted as shown in the `ldapsrequest.inf` example that follows. Make sure you replace the CN placeholder in this example with the FQDN of your DC.

```
-----ldapsrequest.inf -----
[Version]
    Signature="$Windows NT$"
[NewRequest]
    Subject = "CN=<Domain Controller's FQDN>"
    ; replace with the FQDN of the DC
   KeySpec = 1
    KeyLength = 1024
    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
-----
```

2. Generate the LDAPS certificate request file (`ldapsrequest.req`) by typing the following at the command line:

```
Certreq new ldapsrequest.inf ldapsrequest.req
```

- Submit the `ldapsrequest.req` file to the CA of your choice. The CA can then generate the certificate. The CA must return the LDAPS certificate in a Base64-encoded format.

How you submit the request to the CA depends upon the CA you're using. When you're using a Windows standalone CA, you can paste the request in the Saved Request portion of the Submit a Certificate Request or Renewal Request page of the CA enrollment Web pages (as Figure 4-4 illustrates). If you're using a commercial CA (e.g., <http://www.thawte.com>, <http://www.verisign.com>), refer to the enrollment instructions outlined on the CA's Web site.

Figure 4-4

Pasting the LDAPS certificate request in the Enrollment Web Pages of a Windows standalone CA

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page on the Microsoft Certificate Services website. The page has a blue header with 'Microsoft Certificate Services -- RootCA' and a 'Home' link. The main heading is 'Submit a Certificate Request or Renewal Request'. Below this, there is a paragraph explaining that users should paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request into the 'Saved Request' box. The 'Saved Request' section contains a text area with a Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7) and a 'Browse for a file to insert...' link. Below this is the 'Certificate Template' section with a dropdown menu set to 'Administrator'. The 'Additional Attributes' section has an empty text area. At the bottom right, there is a 'Submit >' button.

- Install the LDAPS certificate in the Local Computer certificate store of the DC by typing the following at the command line (`ldaps.cer` is the name of the new LDAPS certificate that was generated by the CA):


```
Certreq accept ldaps.cer
```
- Verify that the LDAPS certificate has been installed in the DC's Local Computer certificate store.

Testing LDAP over SSL for AD

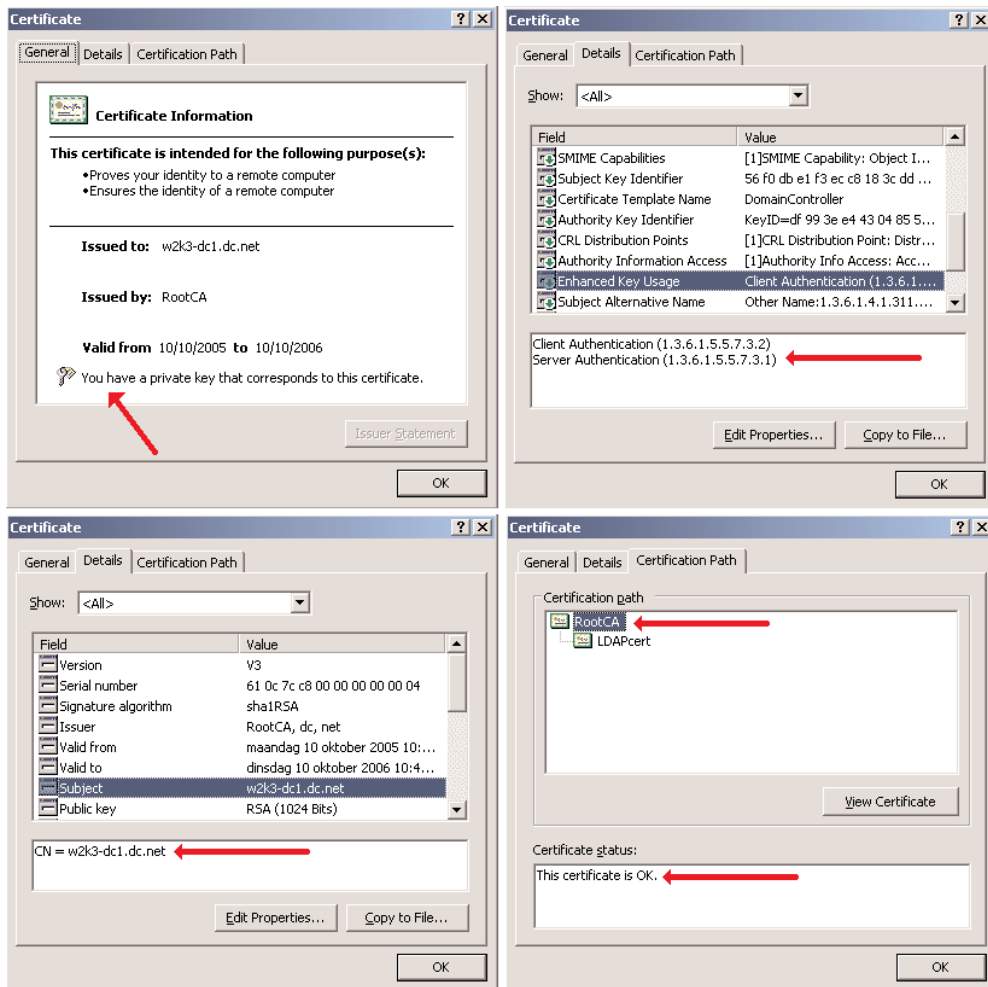
You can validate most of the LDAPS certificate characteristics that we mentioned in the previous section by checking the properties of the certificate in the built-in Windows certificate viewer. If, for example, we open the certificate named `LDAPcert` in the MMC Windows Certificate snap-in (the

one that is selected in Figure 4-2 earlier in the chapter), we can validate the following certificate characteristics (illustrated in Figure 4-5 that follows; the red arrows point to the important elements in these screens):

- The private key associated with the LDAPS certificate is stored in the Personal Certificates store of the Local Computer (upper-left screen of Figure 4-5).
- The LDAPS certificate carries the server authentication OID in the Enhanced Key Usage certificate field (upper-right screen of Figure 4-5).
- The LDAPS certificate carries the DC's FQDN in the Subject certificate field (lower-left screen of Figure 4-5).
- The LDAPS certificate has been issued by a trusted CA (lower-right screen of Figure 4-5).

Figure 4-5

Validating an LDAPS certificate using the built-in Windows certificate viewer



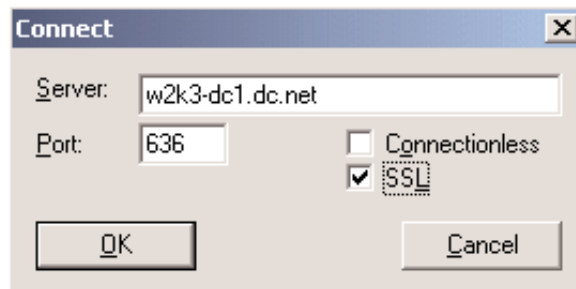
The easiest way to check LDAPS connectivity is to use the LDP.exe utility that comes with the Windows 2000 and Windows Server 2003 Support Tools. More information about using LDP.exe is available from the Microsoft TechNet article entitled “Browsing and Querying Using the LDP Utility” (available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;255602>).

To do the LDP test, follow these steps:

1. Start Ldp.exe.
2. On the Connection menu, click Connect.
3. Type the FQDN of the domain controller to which you want to connect.
4. Type 636 as the port number.
5. Check the SSL box (as Figure 4-6 illustrates). If you don't check this box, the LDP utility will attempt to establish a plain LDAP connection to the DC on port 636.

Figure 4-6

Connecting to the LDAP server over LDAPS using LDP.exe



6. Click OK.

When LDAPS has been configured correctly, you should get a response similar to the one illustrated in Figure 4-7.

Figure 4-7

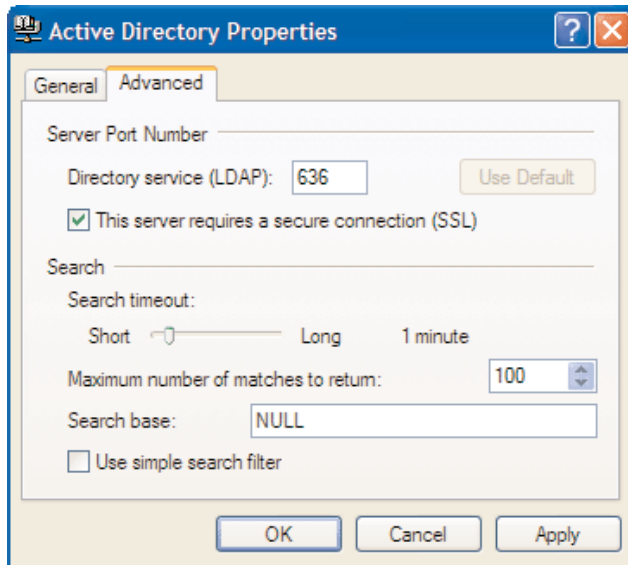
Successful LDAPS connection using LDP.exe



When you connect to an LDAPS-enabled server, you must use the server's FQDN as it is listed in the LDAPS certificate (in the Subject and/or Subject Alternative Name fields, as explained previously), not a DNS alias or IP address. The basis for this requirement is that the LDAP client will check the hostname specified in the connection request to ensure that the hostname matches the name stored in the certificate that is presented by the LDAPS server during the SSL handshake. The LDAPS connection will fail if these two names don't match.

To test LDAPS connectivity, you can also use an LDAPS-enabled client. A good example of such a client is the LDAP client that comes with Microsoft Outlook Express. To communicate using LDAPS with an LDAP server, you must configure the properties of the LDAP server's Outlook Express account. To access the Internet Accounts dialog box, select Accounts... from the Outlook Express Tools menu option. Then open the Properties dialog box of your LDAP server (or Directory Service), and go to the Advanced tab. To configure LDAPS, select the "This server requires a secure connection (SSL)" check box (as Figure 4-8 illustrates).

Figure 8:
Configuring LDAPS in Microsoft Outlook Express



More information about setting up and troubleshooting LDAPS in a Windows DC environment is also available from the following Microsoft Knowledge Base articles:

- "How to Enable LDAP over SSL with a Third-Party Certification Authority" (available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>)
- "You Cannot Reach a Domain Controller on Port 636 with the IP Address Using LDP.exe" (available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;814662>)
- "Unable to Connect to a Domain Controller by Using LDAP Connection over SSL" (available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;296975>)

Leveraging SSL for Secure SMTP

SMTP (Simple Mail Transfer Protocol) is the de facto standard for sending email messages between different messaging servers. SMTP is used not only for server-to-server but also for client-to-server mail communications. In the latter case, SMTP is used to send mail to the server, and the POP3 (Post Office Protocol version 3) or IMAP4 (Internet Message Access Protocol version 4) protocols are used to retrieve mail from the server. The SMTP protocol is defined in RFC 2821, “Simple Mail Transfer Protocol,” which you can download from <http://www.ietf.org/rfc>. SMTP uses the default communication port TCP/25.

By default, SMTP is an insecure protocol: It doesn’t offer authentication, access control, or data-integrity and confidentiality-protection services. Some messaging scenarios, however, do require security. For example, you might not want every Internet user to relay email through your SMTP server, so you choose to restrict this option to only your authorized enterprise users. Today’s messaging servers, however, do offer security features to enhance SMTP security. For example, Exchange Server 2003, Microsoft’s messaging server, lets you authenticate SMTP users via either basic authentication or integrated Windows authentication (either NTLM- or Kerberos-based authentication). Exchange Server 2003 also lets you use the SSL/TLS protocols to provide confidentiality and integrate services for the SMTP traffic. You also need the SSL/TLS protocols to secure the transport of the base64-encoded user credentials when you’re using basic authentication (see chapter 2 of this eBook for more information about basic authentication).

Typically, you access the SMTP over SSL implementation in today’s messaging servers (including Exchange Server 2003) using the standard SMTP port TCP/25. Using this port for access lets servers and clients that do not support SSL still connect to your messaging server, while it also allows servers and clients that do support SSL to switch to a secured SMTP connection. To switch to a secured connection, SMTP uses the StartTLS verb. To stop the secured connection, it uses the StopTLS verb.

In the next sections, we illustrate SMTP SSL/TLS configuration in an Exchange Server 2003/Microsoft Internet Information Server 6.0 (IIS 6.0) environment (IIS 6.0 is the Web server included with Windows Server 2003). In Exchange Server 2003, you can also use SSL/TLS to secure other messaging protocols such as POP3 and IMAP4. A discussion of these protocols in this context, however, is beyond the scope of this eBook.

Setting up SMTP over SSL for Exchange Server 2003

Setting up SMTP over SSL for Exchange Server 2003 is relatively easy and quite similar to setting up LDAPS for AD. Obviously, before you begin, you must have an SSL certificate set up for your Exchange SMTP virtual server.

The SMTP over SSL certificate requirements are identical to the LDAPS certificate requirements we discussed earlier in the chapter:

- The SMTP over SSL certificate must be stored in the Local Computer’s Personal Certificates store of your Exchange SMTP virtual server.
- The private key associated with the SMTP over SSL certificate must be stored in the Local Computer’s private key store.
- The private key associated with the SMTP over SSL certificate must not have strong private-key protection enabled.

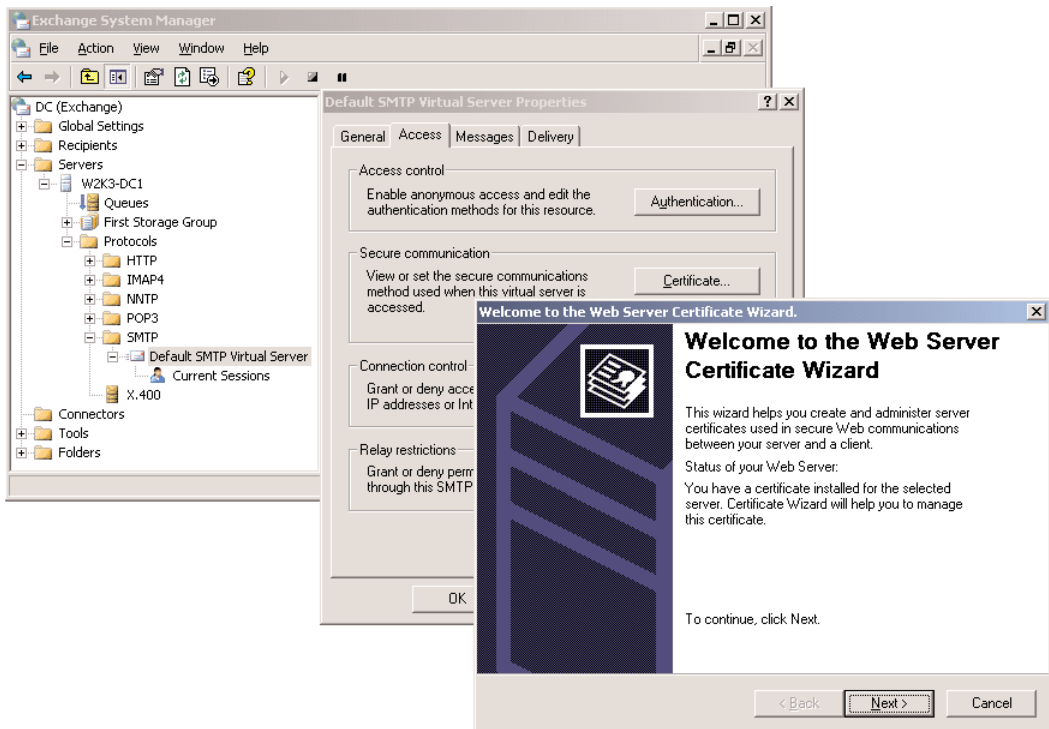
- The Enhanced Key Usage extension of the SMTP over SSL certificate must include the Server Authentication (1.3.6.1.5.5.7.3.1) OID.
- The FQDN of the SMTP virtual server must appear in one of the following X.509 certificate fields of the SMTP over SSL certificate:
 - The CN in the Subject X.509 field.
 - The DNS entry in the Subject Alternative Name X.509 extension.
- The SMTP over SSL certificate must be issued by a CA that the Exchange Server and SMTP clients trust.

To enroll for an SSL certificate, you can use the Certificate Request Wizard, the Windows CA Web enrollment interface, or the certreq.exe command-line utility.

You can start the Certificate Request Wizard from the MMC Exchange System Manager (ESM) snap-in. To do this, go to the Access tab in the Properties dialog box of your SMTP virtual server, and in the Secure Communication section, click the Certificate... button (as Figure 4-9 illustrates).

Figure 4-9

Starting the Certificate Request Wizard from the MMC Exchange System Manager snap-in



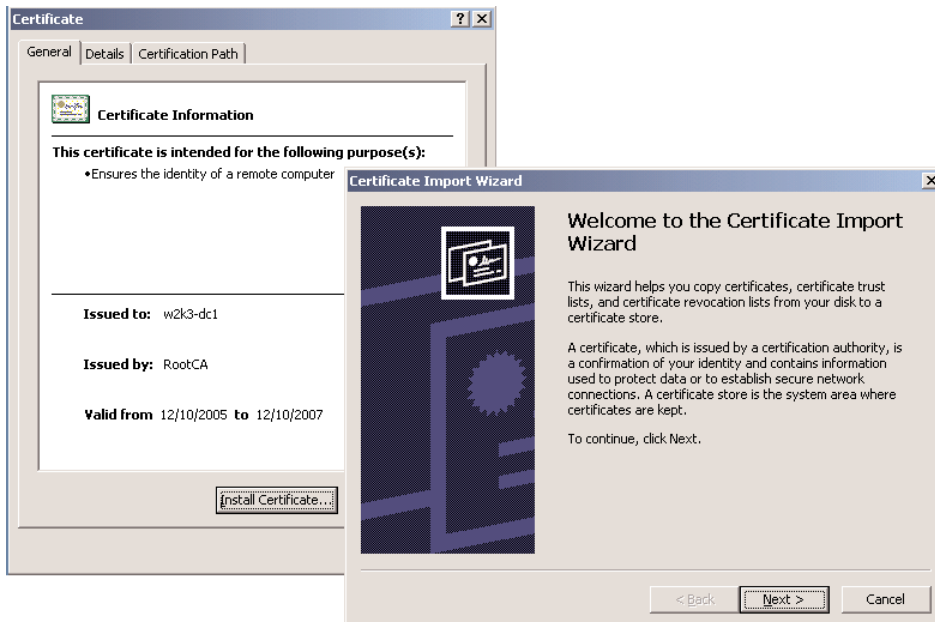
Using the Wizard, you can send the certificate request immediately to an online Windows enterprise CA, or you can save it to a certificate request file. If you save the request, you can either manually submit the saved certificate request file to a standalone Windows CA using the standalone CA Web enrollment pages (as we explained earlier in the “Setting Up LDAP over SSL for AD” section), or you can submit the request to a commercial CA (e.g., Thawte, Verisign). And as noted previously, the commercial CA’s enrollment procedures are detailed on the CA’s Website. Finally, when you request a certificate from a commercial CA, make sure that the CA returns the certificate in a Base64-encoded format.

When you submit the certificate request to an online enterprise CA, the SMTP over SSL certificate will be installed automatically in the Personal Certificates store of the Local Computer. In all other cases, you must manually install the certificate in the Personal Certificates store. An easy way to do this is to use the `certreq.exe` command line with the `-accept` switch (we also explained this method in the LDAPS section). Alternatively, you can install the certificate from the Windows GUI using the Certificate Import Wizard:

1. To start the Certificate Import Wizard (illustrated in Figure 4-10), double-click the certificate file (*.cer) extension, which will bring up the certificate viewer.

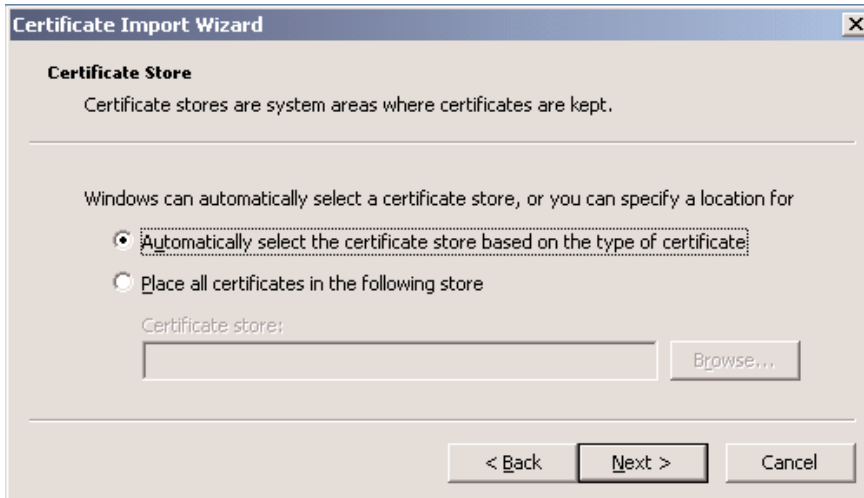
Figure 4-10

Starting the Certificate Import Wizard



2. At the bottom of the viewer, click the Install Certificate... button to start the Import Wizard.
3. In the Wizard, make sure that you select the “Automatically select certificate store based on certificate type” option (as Figure 4-11 illustrates).

Figure 4-11
Selecting the certificate store in the Certificate Import Wizard



When you enroll for an SMTP over SSL certificate using a CA's Web enrollment pages, you must make sure you select the Web Server certificate type. All other steps are similar to the ones outlined in the LDAPS section.

The procedure to enroll for an SMTP over SSL certificate using the certreq.exe command line also is similar to the procedure outlined above for requesting an LDAPS certificate. Just make sure you enter the FQDN of your Exchange SMTP virtual server in the request file.

Configuring SMTP over SSL for Exchange Server 2003

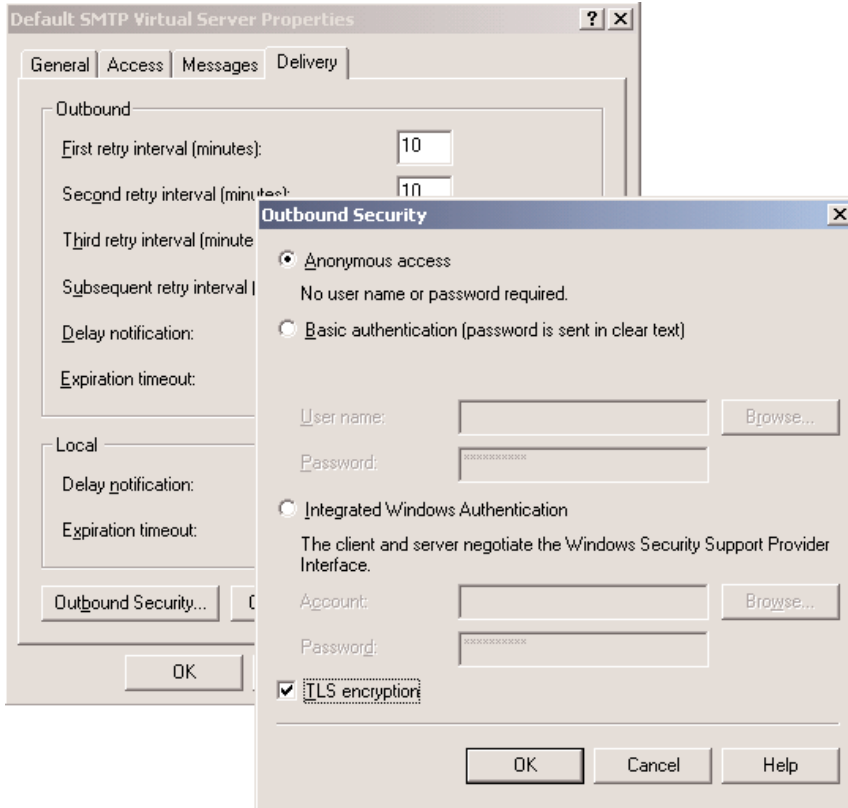
In Exchange Server 2003, you have three options for how to configure SMTP over SSL:

1. You can force the use of SMTP over SSL for all outbound mail.
2. You can force the use of SMTP over SSL only for selected outbound mail domains.
3. You can force the use of SMTP over SSL for all inbound mail.

To force the use of SMTP over SSL for all outbound mail, you must select the "TLS encryption" check box in the Outbound Security properties screen of your SMTP virtual server (as Figure 4-12 illustrates).

Figure 4-12

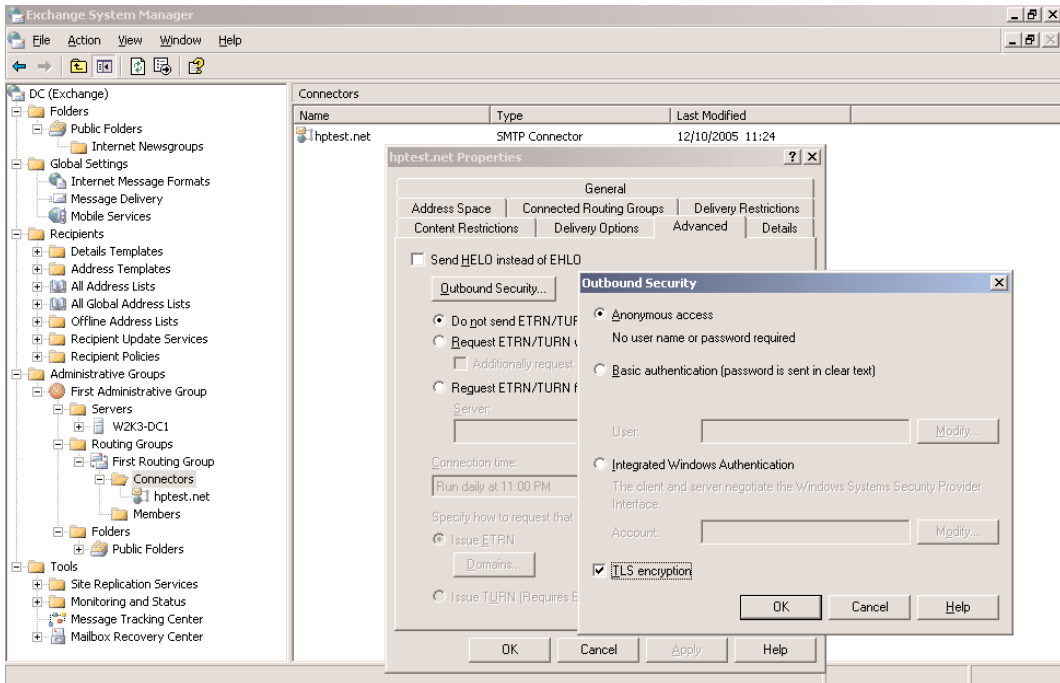
Accessing the Outbound Security properties dialog box from the Exchange System Manager



You can access the Outbound Security properties screen from the SMTP Virtual Server Properties dialog box in the ESM: Select the Delivery tab, and then click the Outbound Security... button. If you enable TLS encryption in the Outbound Security properties dialog box, you restrict your Exchange Server to communicate only with SMTP servers that have SMTP over SSL enabled. A better option is to force SMTP over SSL only for selected outbound mail domains.

Enforcing SMTP over SSL only for selected outbound mail domains ensures that you enforce SSL to the mail domains that effectively support it. To set up this option in Exchange Server 2003, you must define separate SMTP connectors for the different SMTP mail domains to which your Exchange Server is connecting. In the Properties dialog box of the SMTP connector, you then enable/disable SMTP over SSL as needed. This process is illustrated in Figure 4-13.

Figure 4-13
Enabling SMTP over SSL/TLS only for selective SMTP outbound domains, from the Exchange System Manager

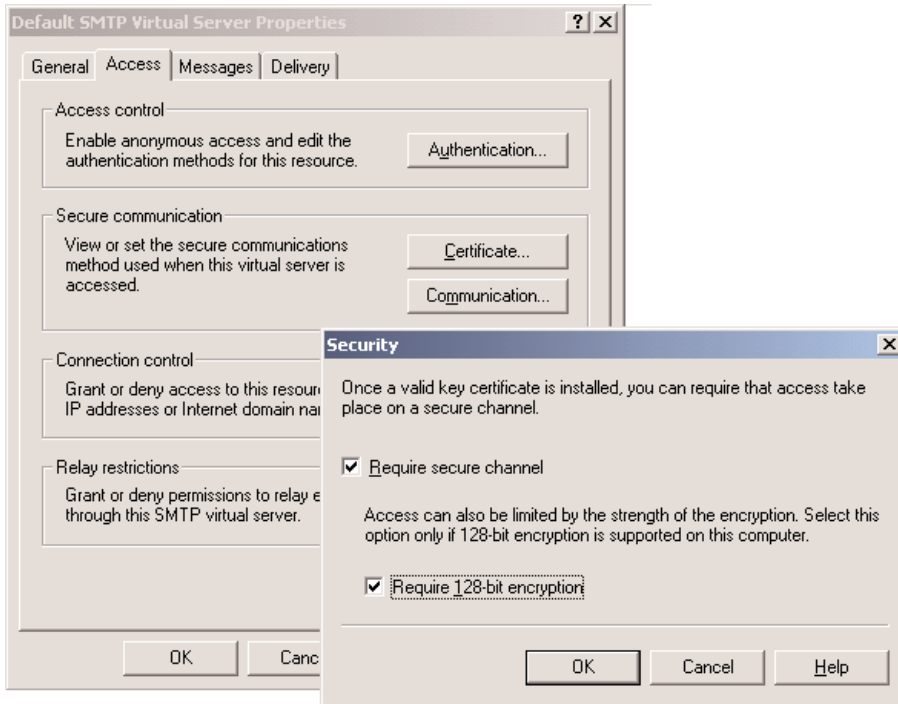


In this example, SMTP over SSL/TLS is enabled only for communication with the messaging servers in the hptest.net SMTP domain. To enable SSL/TLS, select the TLS encryption checkbox in the Outbound Security properties screen that you can access from the Advanced tab in the Properties dialog box of the SMTP connector. By default, the Exchange System Manager does not display routing groups; to display them, you must select the “Display routing groups” option in the Properties dialog box of your Exchange Organization object in the ESM. To access these properties, right-click your Exchange Organization object in the ESM, and select Properties. In Figure 4-13, the Exchange Organization object is labeled DC (Exchange).

You can select the settings to enforce the use of SMTP over SSL for all inbound mail messages from the Access tab in the Default Virtual Server Properties dialog box of your SMTP virtual server. Click the Communication... button, and then select the “Require secure channel” check box (as Figure 4-14 illustrates).

Figure 4-14

Enforcing SMTP over SSL/TLS for all inbound SMTP traffic, from the Exchange System Manager



By default, Exchange negotiates 40-bit key SMTP over SSL encryption. To date, the recommendation is to use 128-bit encryption, so you must also select the “Require 128-bit encryption” check box to follow this advice. After you enable this setting, messaging servers that do not support SMTP over SSL won’t be able to deliver messages to your Exchange Server 2003 SMTP gateway. Note that Exchange does not include an option to enforce SMTP over SSL only for selective inbound SMTP domains (as it does for outbound domains).

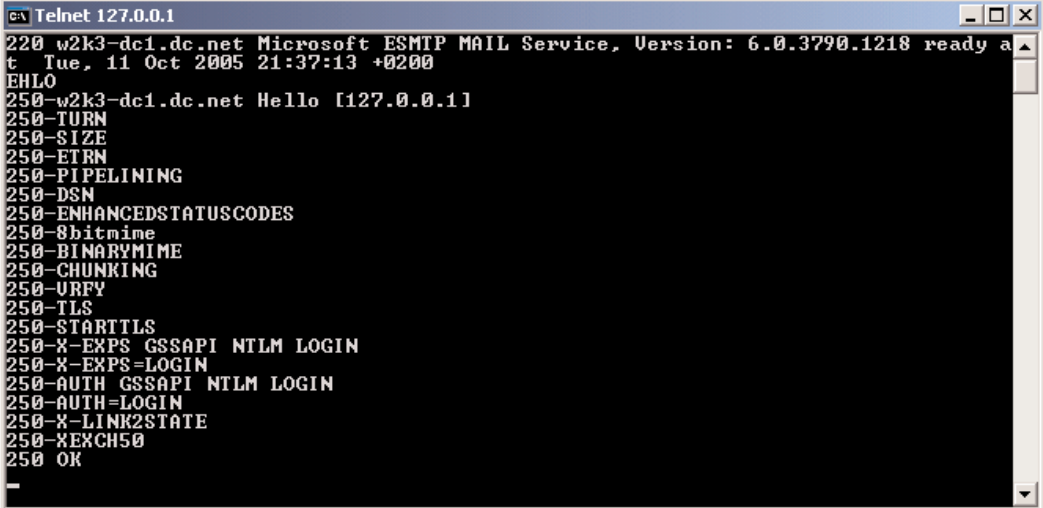
Testing SMTP over SSL for Exchange Server 2003

The easiest way to test whether a messaging server supports SMTP over SSL/TLS is by using the EHLO command. This command returns all SMTP commands supported by an SMTP-enabled messaging server. To do the test, simply type the following text at the command line (and make sure you replace the server-name variable):

```
telnet <messaging server name or IP address> 25
EHLO
```

If SMTP over SSL/TLS is available, the resulting list should contain the STARTTLS command. Figure 4-15 shows a sample output of the EHLO command.

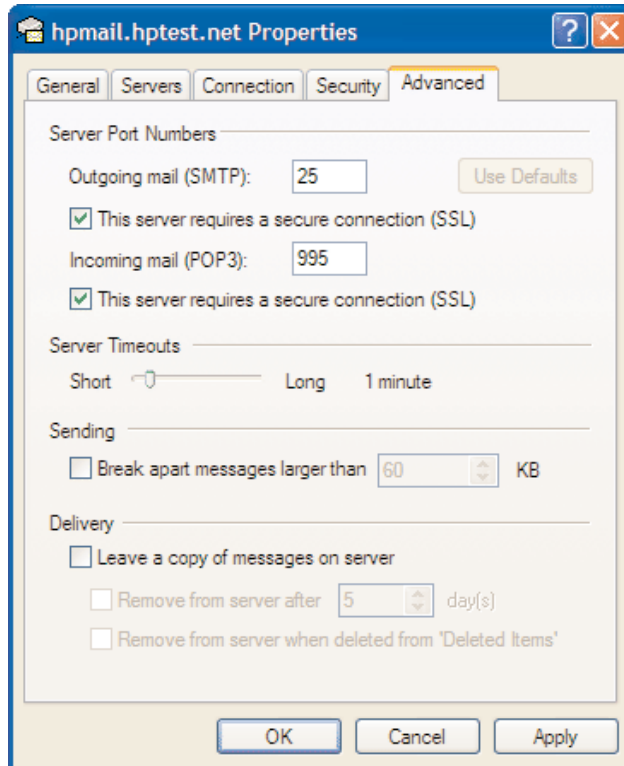
Figure 4-15
Checking StartTLS support using Telnet

A screenshot of a Telnet window titled "Telnet 127.0.0.1". The window shows a list of SMTP capabilities supported by the server. The text is as follows:

```
220 w2k3-dc1.dc.net Microsoft ESMTPL MAIL Service, Version: 6.0.3790.1218 ready a
t Tue, 11 Oct 2005 21:37:13 +0200
EHLO
250-w2k3-dc1.dc.net Hello [127.0.0.1]
250-TURN
250-SIZE
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-URFY
250-TLS
250-STARTTLS
250-X-EXPS GSSAPI NTLM LOGIN
250-X-EXPS=LOGIN
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-X-LINK2STATE
250-REXCH50
250 OK
```

To test SMTP-over-SSL connectivity, you can use an SMTPS-enabled client, such as the SMTP client that comes with Microsoft Outlook Express. To use SMTPS with an SMTP messaging server to communicate, you must configure the properties of the messaging server's Outlook Express account. To access the Internet Accounts dialog box, select Accounts... from the Outlook Express Tools menu option. Then open the Properties dialog box of your messaging server (or "Mail" account), and go to the Advanced tab. To configure SMTPS, select the "This server requires a secure connection (SSL)" checkbox (as Figure 4-16 illustrates).

Figure 4-16
Configuring SMTPS in Outlook Express



More information about setting up and troubleshooting SMTP over SSL/TLS in a Microsoft Exchange environment is also available from the following Microsoft Knowledge Base articles:

- “How to Help Secure SMTP Client Message Delivery in Exchange 2003” (available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;823019>).
- “Securing SMTP Virtual Servers (IIS 6.0)” (available online at <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/8ed22670-c66c-4295-be8b-3335b4eee45c.mspx>).

Leveraging SSL for Secure NNTP

NNTP is the predominant protocol for managing and posting notes on newsgroups. NNTP is defined in RFC 977, “Network News Transfer Protocol: A Proposed Standard for the Stream-Based Transmission of News” (available online from <http://www.ietf.org>).

By default, NNTP is an insecure protocol: It doesn’t provide authentication or data-confidentiality and integrity-protection services. If you look at what NNTP is typically used for—public newsgroups holding notes that everyone can read—security might indeed be considered an afterthought. But you

also can use NNTP to communicate with enterprise newsgroups or newsgroups that contain confidential information, and in those use cases, security becomes very important.

Most NNTP implementations do include security features. The Exchange Server 2003 NNTP service, for example, supports different authentication methods (basic authentication or integrated Windows authentication—NTLM or Kerberos) and data-confidentiality and integrity-protection services that are based on the SSL/TLS protocols. Use of the SSL/TLS protocols in this context is referred to as NNTP over SSL, or Secure News (SNEWS). Standard NNTP typically uses TCP/119 to communicate with the NNTP server. NNTP over SSL typically uses TCP/563 (as summarized in Table 4-2).

Table 4-2 NNTP-related ports

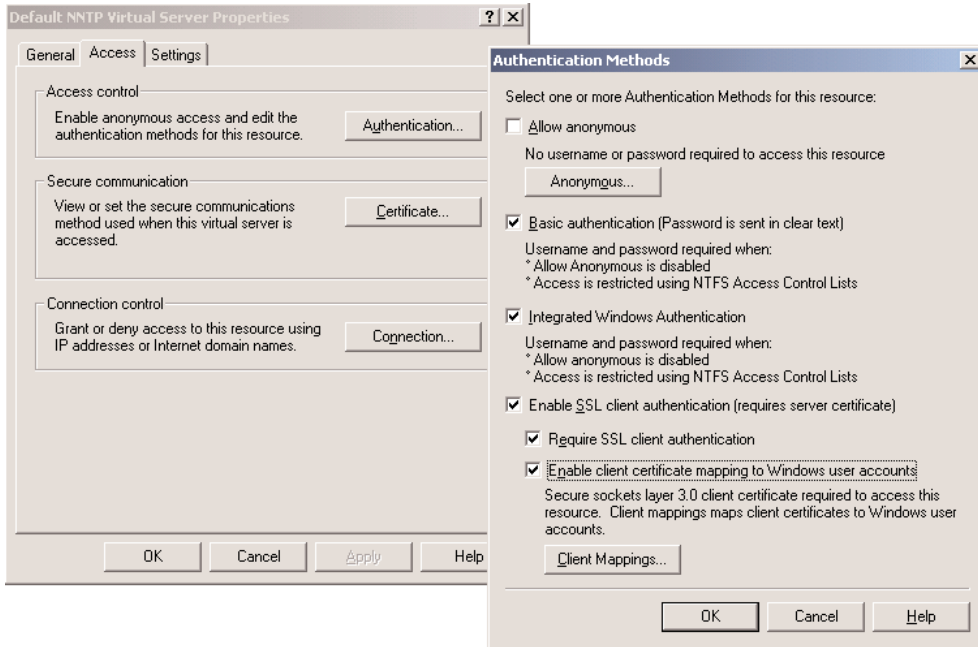
Function/Protocol	Port Number
NNTP	TCP/119
NNTP over SSL (NNTPS)	TCP/563

You can configure the security settings of the Exchange Server 2003 NNTP service from the Properties dialog box of an NNTP virtual server (as Figure 4-14 illustrates for the Default NNTP Virtual Server).

To enable NNTP over SSL, you must always set up an SSL server certificate for the machine that is hosting your NNTP service. To obtain an SSL server certificate, you can use the Web Server Certificate Wizard that you can access by clicking the Certificate... pushbutton in the Access tab of the NNTP Virtual Server Properties dialog box. You can also use any of the certificate enrollment methods outlined previously in this chapter, in the sections on LDAPS and SMTP over SSL.

In Exchange Server 2003, you can also enforce NNTP client certificate-based authentication. You can do this from the Authentication dialog box that is illustrated in Figure 4-17.

Figure 4-17
Configuring NNTP over SSL in the Exchange System Manager

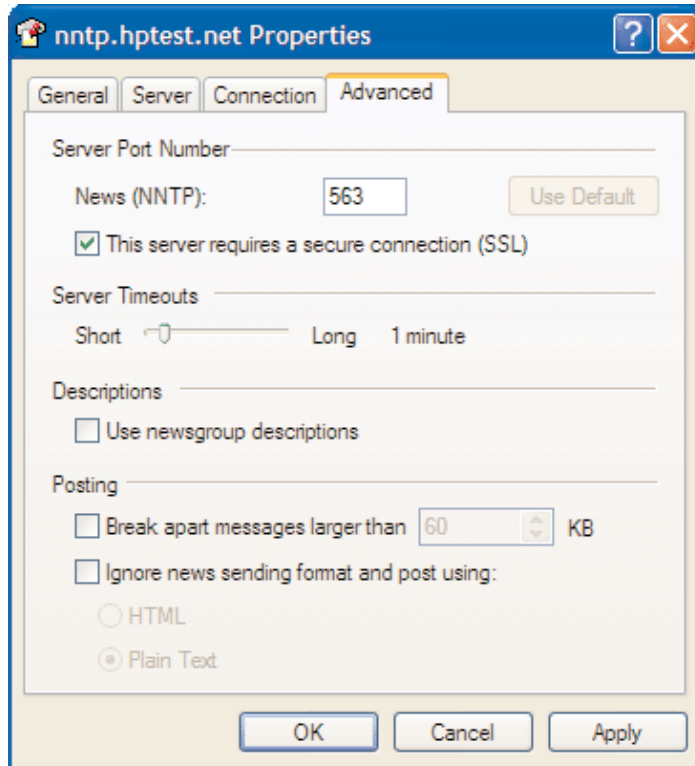


From this box, you can configure the following NNTP over SSL-related settings:

- Enable SSL client authentication—This configuration enables NNTP client authentication using SSL/TLS client certificates.
- Require SSL client authentication—This arrangement requires NNTP clients to provide an SSL/TLS client certificate.
- Enable client certificate mapping to Windows user accounts—This service maps SSL/TLS client certificates to Windows accounts. Access to NNTP data can then be controlled using standard Windows accounts. NNTP over SSL supports both many-to-one and one-to-one mappings. This configuration is similar to the certificate-mapping feature of the HTTPS implementation in the Microsoft Web server (IIS), which we explained in detail in chapter 2 of this eBook.

To test NNTP-over-SSL connectivity, you can use an NNTPS-enabled client. A good example of such a client is the NNTP client that comes with Microsoft Outlook Express. To communicate using NNTPS with an NNTP news server, you must configure the properties of the news server's Outlook Express account. To access the Internet Accounts dialog box, select Accounts... from the Outlook Express Tools menu option. Then open the Properties dialog box of your news server (or "News" account), and go to the Advanced tab. To configure NNTPS, select the "This server requires a secure connection (SSL)" checkbox (illustrated in Figure 4-18).

Figure 4-18
Configuring NNTPS in Outlook Express



Conclusion

This chapter illustrates the flexibility and strength of the SSL/TLS protocols to secure application-layer protocols. The LDAPS, SMTPS, and NNTPS examples here show, once again, the complexity of configuring SSL and the importance of thorough planning and design.