



iSeries

Secure Sockets Layer (SSL)

Version 5 Release 3





iSeries

Secure Sockets Layer (SSL)

Version 5 Release 3

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 19.

Fifth Edition (August 2005)

This edition applies to version 5, release 3, modification 0 of the IBM Operating System/400 (program number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 2002, 2004. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Secure Sockets Layer (SSL)	1
What's new for V5R3	1
Print this topic.	1
Scenarios	2
Scenario: Secure a client connection to your Management Central server with SSL	2
Scenario: Secure all connections to your Management Central server with SSL	5
Concepts	12
History of SSL	12
How SSL works	12
Supported SSL and Transport Layer Security (TLS) protocols	13

Server authentication	14
Client authentication	15
Plan for SSL enablement	15
Secure applications with SSL	16
Troubleshoot SSL	16
Related information	17

Appendix. Notices	19
Trademarks	20
Terms and conditions for downloading and printing publications	20

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) has become an industry standard for enabling applications for secure communication sessions over an unprotected network, such as the Internet. Use the following links to find more information about SSL and your iSeries™ server applications:

- **What's new for V5R3**
makes note of new functions or new information that is available to you, regarding SSL.
- **SSL scenarios**
are a new addition to the SSL information, and are designed to increase your understanding of SSL on the iSeries server by providing possible examples of how SSL can work for you.
- **SSL concepts**
includes supplemental information, providing some basic building blocks for the Secure Sockets Layer (SSL) protocols.
- **Plan for SSL enablement**
includes the prerequisites of SSL enablement on the iSeries server, as well as some helpful tips.
- **Secure applications with SSL**
includes a list of applications that you can secure with SSL on the iSeries server.
- **Troubleshoot SSL**
offers a basic guide for how to begin the procedure of troubleshooting SSL on the iSeries server.
- **Related information for SSL**
includes links to additional information resources for your use.

What's new for V5R3

There are two new items to note, regarding Secure Sockets Layer (SSL) this release:



1. Scenario: Secure a client connection to your Management Central server with SSL
This is a new scenario which explains how to use SSL to secure the connection between a remote client and the Management Central server on an iSeries server, that is the specified central system for a Local Area Network (LAN).
2. GSKit 6B version of GSKit APIs
Starting with V5R3, The GSKit APIs are based on the GSKit 6B version. In the previous release, they were based on the GSKit 4D version. Click here for more information about GSKit APIs.

To find other information about what is new, or has been changed this release, see the Memo to Users



How to see what is new or changed:

To help you see where we made technical changes, this information uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

Print this topic

You can view or download the PDF version of this information. To do so, select Secure Sockets Layer (SSL) (about 243 KB).

Other information:


You can also view or print any of the related information for this topic.

Save PDF files:

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser.
2. Click **Save Target As**.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Download the Adobe Acrobat Reader:

If you need Adobe Acrobat Reader to view or print this information, you can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html). .

Scenarios

The following scenarios are designed to help you maximize the benefits of enabling SSL on your iSeries server:

- Scenario: Secure a client connection to your Management Central server with SSL
This scenario explains how to use SSL to secure the connection between a remote client and an iSeries server that is acting as a central system by using the iSeries Navigator Management Central server.
- Scenario: Secure all connections to your Management Central server with SSL
This scenario explains how to use SSL to secure **all** connections with an iSeries server that is acting as a central system by using the iSeries Navigator Management Central server.
- Scenario: Secure FTP with SSL
This scenario explains how to enable SSL for the FTP application.
- Scenario: Secure Telnet with SSL
This scenario explains how to enable SSL for the Telnet application.
- Scenario: Enhance iSeries SSL performance
This scenario explains how to utilize cryptographic hardware to enhance SSL performance on an iSeries server.
- Scenario: Protect private keys with cryptographic hardware
This scenario explains how to use cryptographic hardware to protect private keys that are associated with SSL transactions on the iSeries server.

Scenario: Secure a client connection to your Management Central server with SSL



Situation:

A company has a local area network (LAN) that includes several iSeries servers in their office. This company's system administrator, Bob, has specified one of the iSeries servers as the central system (hereafter referred to as System A) for the LAN. Bob uses the Management Central server on System A to manage all of the other endpoints on his LAN.

Bob is concerned about connecting to the Management Central server on System A from a network connection that is external to his company's LAN. Bob travels for work a lot, and requires a secure connection to the Management Central server while he is away. He wants to ensure the connection between his PC and the Management Central server is secure when he is not in the company office. Bob decides to enable SSL on his PC and on the System A's Management Central server. With SSL enabled in this way, Bob can be certain that his connection to the Management Central server is secure when he is traveling.

Objectives:

Bob wants to secure the connection between his PC and the Management Central server. Bob does not require additional security for the connection between the Management Central server on System A and the endpoints that are on the LAN. Other employees that work from the company office do not need additional security for their connections to the Management Central server, either. Bob's plan is to configure his PC and the Management Central server on System A, so that his client connection uses server authentication. Connections to the Management Central server from other PCs or iSeries servers on the LAN are not secured with SSL.

Details:

The following table illustrates the types of authentication used, based on the enabling or disabling of SSL on a PC client:

Table 1. Required elements for an SSL-secured connection between a client and the Management Central server

SSL status on Bob's PC	Specified authentication level for the Management Central server on System A	SSL connection enabled?
SSL off	Any	No
SSL on	Any	Yes (server authentication)

Server authentication means that Bob's PC authenticates the Management Central server's certificate. Bob's PC acts as an SSL client when connecting to the Management Central server. The Management Central server acts as an SSL server and must prove its identity. The Management Central server does this by providing a certificate issued by a Certificate Authority (CA) that Bob's PC trusts.

Prerequisites and assumptions:

Bob must perform these administration and configuration tasks in order to secure the connection between his PC and the Management Central server on System A:

1. System A meets the prerequisites for SSL (see SSL Prerequisites).
2. V5R3 (or a later version) of OS/400® is installed on System A. If System A is running V5R1 of OS/400, install the following fixes (PTFs) for OS/400 (5722-SS1):
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. The iSeries Navigator PC client runs V5R3 or later of iSeries Access for Windows®.
4. Get a Certificate Authority (CA) for iSeries servers.
5. Create a certificate that is signed by the CA, for System A.
6. Send the CA and a certificate to System A, and import it into the key database.
7. Assign the certificate with the Management Central server identification.
 - a. On System A, Start IBM® Digital Certificate Manager. Bob obtains or create certificates, or otherwise sets up or changes his certificate system now. See Using Digital Certificate Manager for information on how to set up a certificate system.
 - b. Click **Select a Certificate Store**.
 - c. Select ***SYSTEM** and click **Continue**.
 - d. Enter the ***SYSTEM Certificate Store password**, and click **Continue**. When the menu reloads, expand **Manage Applications**.

- e. Click **Update certificate assignment**.
 - f. Select **Server** and click **Continue**.
 - g. Select the **Management Central Server**, and click **Update certificate assignment**. This assigns a certificate to the Management Central server to use, in order to establish identity to iSeries Access for Windows clients.
 - h. Click **Assign New Certificate**. DCM reloads to the **Update certificate assignment** page with a confirmation message.
 - i. Click **Done**.
8. Set up iSeries Navigator:
 - a. Selectively install the SSL component for iSeries Navigator on the PC client.
 - b. Download the CA to the PC client.

Configuration steps:

Bob needs to complete the following steps in order to secure his PC client connection to the Management Central server on System A, with SSL:

1. Step 1: Deactivate SSL for the iSeries Navigator client
2. Step 2: Set the authentication level for Management Central server
3. Step 3: Restart the Management Central server on System A
4. Step 4: Activate SSL for the iSeries Navigator client
5. Optional step: Deactivate SSL for the iSeries Navigator client

To view the expanded configuration steps, see the following: Secure a client connection to your Management Central server with SSL.

Configuration details: Secure a client connection to your Management Central server with SSL

The following information assumes you have read through the Scenario: Secure a client connection to your Management Central server with SSL. In this scenario, an iSeries server is specified as the central system in a company's local area network (LAN). Bob uses the Management Central server on the central system (referred to here as System A) to manage the endpoints on the company network. The following information explains how to perform the steps required to secure an external client connection to the Management Central server. Follow along as Bob completes the scenario configuration steps.

Before Bob can enable SSL on the Management Central server, he must install the prerequisite programs and set up digital certificates on the iSeries server. See the Prerequisites and assumptions for this scenario before continuing. Once he has met the prerequisites, he can complete the following procedures to enable SSL for the Management Central server.

Step 1: Deactivate SSL for the iSeries Navigator client

1. In iSeries Navigator, expand **My Connections**.
2. Right-click System A and select **Properties**.
3. Click the **Secure Sockets** tab and deselect **Use Secure Sockets Layer (SSL) for connection**.
4. Exit iSeries Navigator and restart it.

The padlock disappears from the Management Central container in iSeries Navigator, indicating an unsecured connection. This indicates to Bob that he no longer has an SSL-secured connection between his client and the central system of his company.

Step 2: Set the authentication level for the Management Central server

1. In iSeries Navigator, right-click **Management Central**, and select **Properties**.
2. Click the **Security** tab, and select **Use Secure Sockets Layer (SSL)**.
3. Select **Any** for the authentication level (available on V5R3 or later of iSeries Access for Windows).

4. Click **OK** to set this value on the central system.

Step 3: Restart the Management Central server on the central system

1. In iSeries Navigator, expand **My Connections**.
2. On **System A**, expand **Network-->Servers** and select **TCP/IP**.
3. Right-click **Management Central** and select **Stop**. The central system view collapses, and a message displays, explaining you are not connected to the server.
4. Once the Management Central server has stopped, click **Start** to restart it.

Step 4: Activate SSL for the iSeries Navigator client

1. In iSeries Navigator, expand **My Connections**.
2. Right-click System A and select **Properties**.
3. Click the **Secure Sockets** tab and select **Use Secure Sockets Layer (SSL) for connection**.
4. Exit iSeries Navigator and restart it.

A padlock appears next to the Management Central server in iSeries Navigator, indicating an SSL-secured connection. This indicates to Bob that he has successfully activated an SSL-secured connection between his client and the central system of his company.

Note: This procedure only secures the connection between one PC and the Management Central server. Other client connections with the Management Central server, as well as connections from endpoints to the Management Central server, will not be secure. To secure other clients, ensure they meet the prerequisites and repeat Step 4. To secure other connections with the Management Central server, see Scenario: Secure all connections to your Management Central server with SSL.

Optional step: Deactivate SSL for the iSeries Navigator client

If Bob wants to work from the company office and does not want an SSL connection affecting the performance of his PC, he can easily deactivate it by performing the following steps:

1. In iSeries Navigator, expand **My Connections**.
2. Right-click **Management Central** and select **Properties**.
3. Click the **Secure Sockets** tab and deselect **Use Secure Sockets Layer (SSL) for connection**.
4. Exit iSeries Navigator and restart it.

The padlock disappears from the Management Central server in iSeries Navigator, indicating an unsecured connection. This indicates to Bob that he no longer has an SSL-secured connection between his PC client and the Management Central server on System A.

See Scenarios for links to other SSL scenarios.

Scenario: Secure all connections to your Management Central server with SSL

Situation:

A company has just set up a wide area network (WAN) that includes several iSeries servers in remote locations (endpoints). The endpoints are centrally managed by one iSeries server (the central system), located at the main office. Tom is the company's security specialist. Tom wants use Secure Sockets Layer (SSL) to secure all of the connections between the Management Central server on the company's central system and all endpoint servers and clients.

Details:

Tom can manage all connections to the Management Central server **securely**, with SSL. To use SSL with the Management Central server, Tom needs to secure iSeries Access for Windows and iSeries Navigator on the PC that he uses to access the central system.

Tom chooses from two authentication levels:

Server authentication

Provides authentication of the endpoint system server certificate. The central system acts as an SSL client when connecting to an endpoint system. The endpoint system acts as an SSL server and must prove its identity by providing a certificate that was issued by a Certificate Authority that the central system trusts. There must be a valid certificate issued by a trusted CA for every endpoint system.

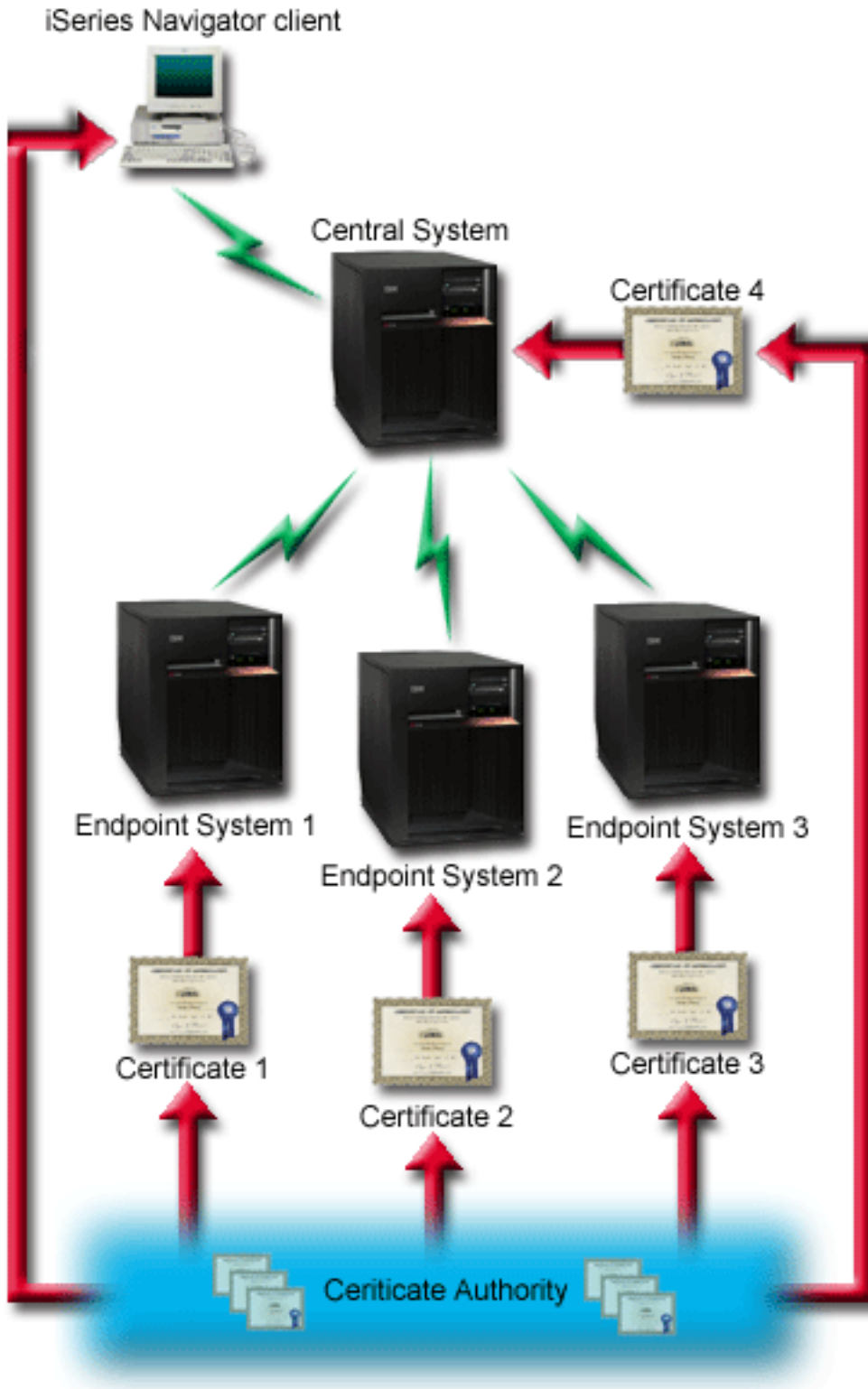
Client and server authentication

Provides authentication of both the central system and the endpoint system certificates. This is a stronger security level than the server authentication level. In other applications, this is known as client authentication, where the client must supply a valid trusted certificate. When the central system (SSL client) attempts to establish a connection with an endpoint system (SSL server), the central system and the endpoint system authenticate each other's certificates for certificate authority authenticity.

Unlike other applications, Management Central also provides authentication through a validation list, called Trusted Group validation list. Generally the validation list stores information that identifies the user, such as a user identification, and authentication information, such as password, personal identification number, or digital certificate. This authentication information is encrypted.

Most applications typically do not specify that you enable both server and client authentication, because server authentication almost always occurs during SSL session enablement. Many applications have client authentication configuration options. Management Central uses the term "server and client authentication" instead of client authentication because of the dual role that the central system plays in the network. When PC users connect to the central system and SSL is enabled, the central system acts as a server. However, when the central system is connecting to an endpoint system, it acts as a client. The following illustration shows how the central system operates as both a server and client in a network.

Note: In this illustration, the certificate associated with the Certificate Authority must be stored in the key database on the central system and on all of the endpoint systems.



Prerequisites and assumptions:

Tom must perform the following administration and configuration tasks (see the image, SSL-secured Management Central WAN), in order to secure all of the connections to the Management Central server:

1. The central system meets the prerequisites for SSL (see SSL Prerequisites).
2. The central system and all endpoint iSeries servers run V5R2 or later versions of OS/400. Install the following fixes (PTFs) for OS/400 (5722-SS1), if the central system and endpoints run V5R1 of OS/400:
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. The iSeries Navigator PC client runs V5R2 or later of iSeries Access for Windows. If the client is at V5R1, install the service pack PTF SI01907 (or later) for V5R1 iSeries Access for Windows (5722-XE1). See the V5R1 Information Center, "Securing Management Central" page for more information.
4. Get a Certificate Authority (CA) for iSeries servers.
5. Create a certificate, signed by the CA, for each iSeries server that is managed by the SSL-enabled Management Central server.
6. Send the CA and a certificate to each iSeries server, and import them into the key database.
7. Assign the certificates with the Management Central application identification, and the application identifications for all of the endpoint servers that iSeries Navigator uses:
 - a. Start IBM Digital Certificate Manager on the central server. If Tom needs to obtain or create certificates, or otherwise setup or change his certificate system, he does so now (see Using Digital Certificate Manager for information on setting up a certificate system).
 - b. Click **Select a Certificate Store**.
 - c. Select ***SYSTEM** and click **Continue**.
 - d. Enter the ***SYSTEM Certificate Store password**, and click **Continue**. When the menu reloads, expand **Manage Applications**.
 - e. Click **Update certificate assignment**.
 - f. Select **Server** and click **Continue**.
 - g. Select the **central system**, and click **Update certificate assignment**. This assigns a certificate to the Management Central server to use, in order to establish identity to iSeries Access for Windows clients.
 - h. Click **Assign New Certificate**. DCM reloads to the **Update certificate assignment** page with a confirmation message.
 - i. Click **Done**.
 - j. Repeat this procedure for all endpoint servers that iSeries Navigator uses.
8. Set up iSeries Navigator:
 - a. Selectively install the SSL component for iSeries Navigator on the PC client.
 - b. Download the CA to the PC client.

Configuration steps:

Before Tom can enable SSL on the Management Central server, he must install the prerequisite programs and set up digital certificates on the central system. See the Prerequisites and assumptions for this scenario before continuing. Once he has met the prerequisites, he can complete the following procedures to secure all connections to the Management Central server:

Note: If SSL has been enabled for iSeries Navigator, Tom must disable it before he can enable SSL on the Management Central server. If SSL has been enabled for iSeries Navigator and not the Management Central server, attempts by iSeries Navigator to connect with the central system will fail.

- Step 1: Configure the central system for server authentication

- Step 2: Configure endpoint systems for server authentication
- Step 3: Restart the Management Central server on the central system
- Step 4: Restart the Management Central server on all endpoint systems
- Step 5: Activate SSL for the iSeries Navigator client
- Step 6: Configure the central system for client authentication
- Step 7: Configure endpoint systems for client authentication
- Step 8: Copy the validation list to the endpoint systems
- Step 9: Restart the Management Central server on the central system
- Step 10: Restart the Management Central server on all endpoint systems

To view the expanded configuration steps, see Configuration details: Secure all connections to your Management Central server with SSL.

Configuration details: Secure all connections to your Management Central server with SSL

The following information assumes that you have read through the following information: Scenario: Secure all connections to your Management Central server with SSL. You now want to understand how to perform the steps required to secure all connections to the Management Central server. Follow along as Tom completes the scenario.

Before Tom can enable SSL on the Management Central server, he must install the prerequisite programs and set up digital certificates on the iSeries server. See the Prerequisites and assumptions for this scenario before continuing. Once he has met the prerequisites, he can complete the following procedures to secure all connections to the Management Central server.

Note: If SSL has been enabled for iSeries Navigator, Tom must disable it before he can enable SSL on the Management Central server. If SSL has been enabled for iSeries Navigator, and not the Management Central server, attempts by iSeries Navigator to connect with the central system will fail.

Step 1: Configure the central system for server authentication

SSL allows Tom to secure transmissions between a central system and an endpoint system, as well as between the iSeries Navigator client and the central system. SSL provides transport and authentication of certificates and encryption of data. An SSL-connection can only occur between an SSL-enabled central system and an SSL-enabled endpoint system. Tom needs to configure server authentication before he can configure client authentication

1. In iSeries Navigator, right-click **Management Central** and select **Properties**.
2. Click the **Security** tab and select **Use Secure Sockets Layer (SSL)**
3. Select **Server** as the authentication level.
4. Click **OK** to set this value on the central system.

Note: Do **NOT** restart the Management Central server until after the configuration of endpoint systems for server authentication is complete.

5. Configure endpoint systems for server authentication.

Step 2: Configure endpoint systems for server authentication

After Tom configures the central system for server authentication, he needs to configure the endpoint systems for server authentication. He completes the following tasks:

1. Expand **Management Central**.
2. Compare and update system values for the endpoint systems:
 - a. Under **Endpoint Systems**, right-click on the central system and select **Inventory—>Collect**.

- b. Check the **System Values** option on the collect dialog, in order to collect the system values inventory for the central system. Deselect any other options.
- c. Right-click **System Groups**—>**New System Group**.
- d. Define a new system group which includes all endpoint systems to connect to, using SSL.
- e. To display the new group, expand the list of system groups.
- f. After the collection is complete, right-click the new system group and select **System Values**—>**Compare and Update**.
- g. Verify that the central system displays in the **Model system** field.
- h. Select the **Management Central** category and verify the following values, checking the box next to each:
 - Specify **Yes**, to **Use Secure Sockets Layer**.
 - Specify **Server** for the SSL authentication level.

You set these values on the central system during the procedure, Configure the central system for server authentication.
- i. Click **OK** to set these values on the endpoint systems in the new system group.
- j. Wait for the **Compare and Update** process to complete before restarting the Management Central server. This may take a few minutes.

Step 3: Restart the Management Central server on the central system

1. In iSeries Navigator, expand **My Connections**.
2. Expand the central system view.
3. Expand **Network**—> **Servers** and select **TCP/IP**.
4. Right-click **Management Central** and select **Stop**. The central system view collapses, and a message displays, explaining that you are not connected to the server.
5. Once the Management Central server has stopped, click **Start** to restart it.

Step 4: Restart the Management Central server on all endpoint systems

1. Expand the endpoint system that you are restarting.
2. Expand **Network**—> **Servers** and select **TCP/IP**.
3. Right-click **Management Central** and select **Stop**.
4. Once the Management Central server has stopped, click **Start** to restart it.
5. Repeat this procedure for each endpoint system.

Step 5: Activate SSL for the iSeries Navigator client

1. In iSeries Navigator, expand **My Connections**.
2. Right-click the central system, and select **Properties**.
3. Click the **Secure Sockets** tab and select **Use Secure Sockets Layer (SSL) for connection**.
4. Exit iSeries Navigator and restart it.

Step 6: Configure the central system for client authentication (optional step)

Now that Tom has completed the configuration for server authentication, he can perform the following optional client authentication procedures. Client authentication provides validation of Certificate Authority and trusted group for both the endpoint systems and the central system. When the central system (SSL client) tries to use SSL to connect to an endpoint system (SSL server), the central system and the endpoint system authenticate each other's certificates through client authentication. This is also referred to as Certificate Authority and Trusted Group authentication.

Note: You cannot complete client authentication configuration until you have configured server authentication.

1. In iSeries Navigator, right-click **Management Central** and select **Properties**.
2. Click the **Security** tab and select **Use Secure Sockets Layer (SSL)**.
3. Select **Client and server** for the authentication level.
4. Click **OK** to set this value on the central system.

Note: Do **NOT** restart the Management Central server until you have configured all endpoint systems to use SSL with client and server authentication.

5. Configure endpoint systems for client authentication.

Step 7: Configure endpoint systems for client authentication (optional step)

1. Compare and update system values for the endpoint systems:

Note: This task does not work for any endpoint iSeries servers that are running V4R5.

- a. Under **Endpoint Systems**, right-click on the central system and select **Inventory—>Collect**.
- b. Check the **System Values** option on the collect dialog, in order to collect the system values inventory for the central system. Deselect any other options.
- c. Right-click **System Groups—>New System Group**.
- d. Define a new system group that includes all the endpoint systems to connect to, using SSL.
- e. To display the new group, expand the list of system groups.
- f. After the collection is complete, right-click the new system group and select **System Values—>Compare and Update**.
- g. Verify that **Management Central server** displays in the **Model System** field.
- h. Select the **Management Central** category and verify the following:
 - Specify **Yes to Use Secure Sockets Layer**.
 - Specify **Client and Server** for the SSL authentication level.

You set these values on the central system during the procedure, Configure the central system for client authentication. Check the **Update** box next to each value.

- i. Click **OK** to set these values on the endpoint systems in the new system group.

Step 8: Copy the validation list to the endpoint systems

1. In iSeries Navigator, expand **Management Central—>Definitions**.
2. Right-click **Package**, and select **New Definition**.
3. In the **New Definition** window, work with the following:
 - **Name:** Type the name of the definition.
 - **Source system:** Select the name of the central system.
 - **Selected files and folders:** Click in the field, and type `/QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL`.
4. Click the **Options** tab, and select **Replace existing file with the file being sent**.
5. Click **Advanced**.
6. In the **Advanced Options** window, specify **Yes** to allow object differences on restore.
7. Click **OK** to refresh the list of definitions and display the new package.
8. Right-click the new package, and select **Send**.
9. In the **Send** dialog: Add the trusted group, remove any others, and click **OK**. The Trusted group is the system group you defined in Step 1 of this procedure.

Note: The **Send** task will always fail on the central system, because it is always the source system. The **Send** task should complete successfully on all endpoint systems.

Step 9: Restart the Management Central server on the central system

1. In iSeries Navigator, expand **My Connections**.
2. Expand the central system.
3. Expand **Network**—> **Servers** and select **TCP/IP**.
4. Right-click **Management Central** and select **Stop**. The central system view collapses, and a message displays, explaining that you are not connected to the server.
5. Once the Management Central server has stopped, click **Start** to restart it.

Step 10: Restart the Management Central server on all endpoint systems

Note: Repeat this procedure for each endpoint system.

1. Expand the endpoint system that you are restarting.
2. Expand **Network**—> **Servers** and select **TCP/IP**.
3. Right-click **Management Central** and select **Stop**.
4. Once the Management Central server has stopped, click **Start** to restart it.

See Scenarios for links to other SSL scenarios.

Concepts

With the SSL protocol, you can establish secure connections between clients and server applications which provide authentication of one or both endpoints of the communication session. SSL also provides privacy and integrity of the data that client and server applications exchange.

Use the following conceptual information gain a better understanding of the relationship between SSL and the iSeries server:

- History of SSL
- How SSL works
- Supported SSL and Transport Layer Security (TLS) protocols
- Server authentication
- Client authentication

History of SSL

Netscape developed The Secure Sockets Layer Protocol (SSL) in 1994, as a response to the growing concern over security on the Internet. SSL was originally developed for securing web browser and server communications. The specification was designed in such a way so you can enable other applications, such as TELNET and FTP, to use SSL. See Supported SSL and Transport Layer Security (TLS) protocols for more information on SSL and related protocols.

How SSL works

SSL is actually two protocols. The protocols are the record protocol and the handshake protocol. The record protocol controls the flow of the data between the two endpoints of an SSL session.

The handshake protocol authenticates one or both endpoints of the SSL session and establishes a unique symmetric key used to generate keys to encrypt and decrypt data for that SSL session. SSL uses asymmetric cryptography, digital certificates, and SSL handshake flows, to authenticate one or both endpoints of an SSL session. Usually, SSL authenticates the server. Optionally, SSL authenticates the client. A digital certificate, issued by a Certificate Authority, can be assigned to each of the endpoints or to the applications using SSL on each endpoint of the connection.

The digital certificate is comprised of a public key and some identifying information that a trusted Certificate Authority (CA) has digitally signed. Each public key has an associated private key. The private key is not stored with or as part of the certificate. In both server and client authentication, the endpoint which is being authenticated must prove that it has access to the private key associated with the public key contained within the digital certificate.

SSL handshakes are performance intensive operations because of the cryptographic operations using the public and private keys. After an initial SSL session has been established between two endpoints, the SSL session information for these two endpoints and applications can be cached in secure memory to speed up subsequent SSL session enablements. When an SSL session is resumed, the two endpoints use an abbreviated handshake flow to authenticate that each has access to unique information without using the public or private keys. If both can prove that they have access to this unique information, then new symmetric keys are established and the SSL session resumes. For TLS Version 1.0 and SSL Version 3.0 sessions, cached information will not remain in the secure memory for greater than 24 hours. In V5R2M0 and subsequent releases, you can minimize SSL handshake performance impacts on the main CPU by using cryptographic hardware.

Supported SSL and Transport Layer Security (TLS) protocols

There are several versions of the SSL protocol defined. The latest version, the Transport Layer Security Protocol (TLS), is based on SSL 3.0 and is a product of the Internet Engineering Task Force (IETF). The OS/400 implementation supports the following versions of the SSL and TLS protocols:

- TLS Version 1.0
- TLS Version 1.0 with SSL Version 3.0 compatibility

Notes:

1. Specifying TLS Version 1.0 with SSL Version 3.0 compatibility means that TLS will be negotiated if possible and if that is not possible then SSL Version 3.0 will be negotiated. If SSL Version 3.0 cannot be negotiated, the SSL handshake will fail.
2. We also support TLS Version 1.0 with SSL Version 3.0 and SSL Version 2.0 compatibility. This is specified with the protocol value of **ALL**, which means that TLS will be negotiated if possible and if that is not possible then SSL Version 3.0 will be negotiated. If SSL Version 3.0 cannot be negotiated, SSL Version 2.0 will be negotiated. If SSL Version 2.0 cannot be negotiated, the SSL handshake will fail.

- SSL Version 3.0
- SSL Version 2.0
- SSL Version 3.0 with SSL Version 2.0 compatibility

SSL Version 3.0 versus SSL Version 2.0


SSL version 3.0 is an almost totally different protocol compared to SSL Version 2.0. Some of the major differences between the two protocols include:

- SSL Version 3.0 handshake protocol flows are different than SSL Version 2.0 handshake flows.
- SSL Version 3.0 uses the BSAFE 3.0 implementation from RSA Data Security, Incorporated. BSAFE 3.0 includes a number of timing attack fixes and the SHA-1 hashing algorithm. The SHA-1 hashing algorithm is considered to be more secure than the MD5 hashing algorithm. SHA-1 allows SSL Version 3.0 to support additional cipher suites which use SHA-1 instead of MD5.
- SSL Version 3.0 protocol reduces man-in-the-middle (MITM) type of attacks from occurring during SSL handshake processing. In SSL Version 2.0, it was possible, though unlikely, that a MITM attack could accomplish cipher specification weakening. Weakening the cipher could allow an unauthorized person to break the SSL session key.

Note: If you want to restrict SSL Version 2.0 on your system, click the **Send feedback** link located at the top of this page and fill out the form with your contact information. In the comments section of the form,

include the following text "I would like instructions on how to restrict SSL Version 2.0 on a system running V5R3 OS/400" and click **Submit**. You will be contacted with further instructions.

TLS Version 1.0 versus SSL Version 3.0

The latest industry standard SSL protocol based on SSL version 3.0 is Transport Layer Security (TLS) Version 1.0. Its specifications are defined by the Internet Engineering Task Force (IETF) in RFC 2246, "The TLS Protocol." 

The major goal of TLS is to make SSL more secure and to make the specification of the protocol more precise and complete. TLS provides these enhancements over SSL Version 3.0:

- A more secure MAC algorithm
- More granular alerts
- Clearer definitions of "gray area" specifications

Any iSeries server applications that are enabled for SSL will automatically obtain TLS support unless the application has specifically requested to use only SSL Version 3.0 or SSL Version 2.0.

TLS provides the following security improvements:

- **Key-Hashing for Message Authentication**
TLS uses Key-Hashing for Message Authentication Code (HMAC), which ensures that a record cannot be altered while travelling over an open network such as the Internet. SSL Version 3.0 also provides keyed message authentication, but HMAC is more secure than the (Message Authentication Code) MAC function that SSL Version 3.0 uses.
- **Enhanced Pseudorandom Function (PRF)**
PRF generates key data. In TLS, the HMAC defines the PRF. The PRF uses two hash algorithms in a way which guarantees its security. If either algorithm is exposed, the data will remain secure as long as the second algorithm is not exposed.
- **Improved finished message verification**
Both TLS Version 1.0 and SSL Version 3.0 provide a finished message to both endpoints that authenticates that the exchanged messages were not altered. However, TLS bases this finished message on the PRF and HMAC values, which again is more secure than SSL Version 3.0.
- **Consistent certificate handling**
Unlike SSL Version 3.0, TLS attempts to specify the type of certificate which must be exchanged between TLS implementations.
- **Specific alert messages**
TLS provides more specific and additional alerts to indicate problems that either session endpoint detects. TLS also documents when certain alerts should be sent.

Server authentication

With server authentication, the client will ensure that the server certificate is valid and that it is signed by a certificate authority (CA) which the client trusts. SSL will use asymmetric cryptography and handshake protocol flows to generate a symmetric key which will be used only for this unique SSL session. This key is used to generate a set of keys which are used for encrypting and decrypting data which will flow over the SSL session. Subsequently, when an SSL handshake has completed, one or both ends of the communication link will have been authenticated. Additionally, a unique key will have been generated to encrypt and decrypt the data. Once the handshake is completed then application layer data will flow encrypted across that SSL session.

Client authentication

Many applications allow the option to enable client authentication. With client authentication, the server will ensure that the client certificate is valid and that it is signed by a Certificate Authority which the server trusts. The following iSeries server applications support client authentication:

- IBM HTTP Server (powered by Apache)
- FTP server
- Telnet server
- Management Central endpoint system
- Directory Services (LDAP)

Plan for SSL enablement

When planning to enable SSL on an iSeries server, consider the following:

- SSL prerequisites
- What type of digital certificates you want, and where to obtain them

SSL Prerequisites:

- IBM Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- If you are trying to use the HTTP server to use the DCM, ensure that you have the IBM Developer Kit for Java™ (5722-JV1) installed. Otherwise, the HTTP admin server will not start.
- The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.

Note: If you want to restrict SSL from supporting less than 128 bits of secret material within the symmetric key, click the **Send feedback** link located at the top of this page and fill out the form with your contact information. In the comments section of the form, include the following text "I would like instructions on how to restrict SSL from supporting less than 128 bits of secret material within the symmetric key on a system running V5R3 OS/400" and click **Submit**. You will be contacted with further instructions.

- You may also want to install cryptographic hardware to use with SSL to speed up the SSL handshake processing. See the Cryptographic hardware information for available options. If you want to install cryptographic hardware, you must also install Option 35, the Cryptographic Service Provider.

If you want to use SSL with iSeries Access for Windows components, you must also install the iSeries Client Encryption product, 5722-CE3 (128-bit). iSeries Access for Windows requires this product in order to establish the secure connection.

Note: You do not need to install a Client Encryption Product to use the PC5250 emulator that is shipped with the Personal Communications product. Personal Communications has its own built-in encryption code.

Digital certificates

See Using public certificates versus issuing private certificates to better understand the differences between public and private digital certificates, and your options for obtaining them.

IBM Digital Certificate Manager (DCM) is the iSeries server solution for managing digital certificates. To find out more about DCM, see the Information Center topic Using Digital Certificate Manager.

Secure applications with SSL

You can secure the following iSeries server applications with SSL:

- Enterprise Identity Mapping (EIM)
- FTP server
- HTTP server (powered by Apache)
- iSeries Access for Windows
- Directory Services Server (LDAP)
- Distributed relational database architecture (DRDA[®]) and distributed data management (DDM) server
- Management Central server
- Telnet server
- Websphere Application Server — Express
- Applications that are written to the iSeries Access for Windows set of APIs (application programming interfaces)
- Applications developed using the secure sockets Application Programmable Interfaces (APIs) supported on the iSeries server. The supported APIs are Global Secure Toolkit (GSKit) and the SSL_iSeries native APIs. See the Secure Sockets APIs for information on both GSKit and SSL_APIs.

Troubleshoot SSL

This very basic troubleshooting information is intended to help you thin out the list of possible problems that the iSeries server can encounter with SSL. It is important to understand that this is not a comprehensive source for troubleshooting information, but simply a guide.

Verify that the following statements are true:

- You have met the prerequisites for SSL on the iSeries server (see SSL Prerequisites).
- If you are using the Management Central technology of iSeries Navigator with a V5R1 system, you have installed the following PTFs on your system:
 - si01375
 - si01376
 - si01377
 - si01378
 - si01838
- Your certificate authority and certificates are valid and have not expired.

If you have verified that the previous statements are true for your system and you still have an SSL-related problem, try the following options:

- The SSL error code in the server job log can be cross referenced in an error table to find more information on the error. See the Secure socket API error code messages page to access information on secure socket error code messages. For example, this table maps the -93 that might be seen in a server job log to the constant `SSL_ERROR_SSL_NOT_AVAILABLE`.
 - A negative return code (indicated by the dash before the code number) indicates that you are using an `SSL_API`.
 - A positive return code indicates that you are using a `GSKit` API. Programmers can code the `gsk_strerror()` or `SSL_strerror()` API in their programs to obtain a brief description of an error return code. Some applications make use of this API and print out a message to the job log containing this sentence.

If more detailed information is required, the message id provided in the table can be displayed on an iSeries server to show potential cause and recovery for this error. Additional documentation explaining these error codes may be located in the individual secure socket API that has returned the error.

- The following two header files contain the same constant names for System SSL return codes as the table, but without the message ID cross reference:

– QSYSINC/H.GSKSSL

–



QSYSINC/H.QSOSSL<<

Remember that although the names of the System SSL return codes remain constant in these two files, more than one unique error can be associated with each return code.

For more troubleshooting information regarding the iSeries server, see the Troubleshooting and service page.



Related information

You can find additional SSL information in the following sources:

IBM Sources

- The SSL and Java Secure Socket Extension (JSSE) page includes a brief description of JSSE and how you can use it.
- The IBM Toolbox for Java page includes a brief description of the Java classes available, and how you can use them.

Request for comments

- RFC 2246: "The TLS Protocol Version 1.0"  explains the TLS protocol in detail.
- RFC2818: "HTTP Over TLS"  describes how to use TLS to secure HTTP connections over the Internet.

Other sources

- The The SSL Protocol Version 3.0 document  explains SSL Protocol Version 3.0 in great detail.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows NT

Lotus[®], Freelance, and WordPro are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft[®], Windows, Windows NT[®], and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for downloading and printing publications

Permissions for the use of the publications you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

Personal Use: You may reproduce these Publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these Publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these Publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these Publications, or reproduce, distribute or display these Publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the Publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

All material copyrighted by IBM Corporation.

By downloading or printing a publication from this site, you have indicated your agreement with these terms and conditions.



Printed in USA