



System i
Networking
E-mail

Version 6 Release 1





System i
Networking
E-mail

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in “Notices,” on page 51.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-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 1998, 2008. All rights reserved.

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

Contents

E-mail	1	Sending e-mail through a router or firewall.	23
What's new for V6R1	1	Prerequisites for an e-mail router	23
PDF file for E-mail	1	Authenticating e-mail for local and relay	24
E-mail concepts	2	Tracking the e-mail sender	24
Simple Mail Transfer Protocol on i5/OS	3	Restricting the relay of messages	25
Post Office Protocol on i5/OS.	4	Accepting relay messages from Post Office	
Scenarios: E-mail	4	Protocol clients	26
Scenario: Sending and receiving e-mail locally	4	Using relay restriction and connection	
Scenario: Configuring the QtmsCreateSendEmail		restriction functions together	26
API to use S/MIME	6	Restricting connections	27
Planning for e-mail	9	Filtering e-mail to prevent virus proliferation	28
Controlling e-mail access	10	Sending and receiving e-mail	28
Controlling Simple Mail Transfer Protocol		Setting up Post Office Protocol e-mail clients	29
access	10	JavaMail	30
Controlling Post Office Protocol access	11	Sending spooled files as PDF files	30
Preventing e-mail access	11	Using Lightweight Directory Access Protocol for	
Preventing Simple Mail Transfer Protocol		addresses	30
access	11	Sending e-mail using Systems Network	
Preventing Simple Mail Transfer Protocol		Architecture distribution services	31
from starting when TCP/IP starts	11	Setting up headers to differentiate between	
Preventing access to Simple Mail Transfer		recipients	31
Protocol ports	12	Supporting Internet addressing for the	
Holding Systems Network Architecture		SNDDST command.	32
Distribution Services queues.	12	Attaching files	33
Preventing Post Office Protocol access	12	Receiving e-mail using Systems Network	
Preventing Post Office Protocol from		Architecture distribution services	33
starting when TCP/IP starts.	12	Managing e-mail	34
Preventing access to Post Office Protocol		Checking e-mail servers	34
ports	13	Removing Post Office Protocol e-mail users.	35
Configuring e-mail	13	Preventing large e-mail messages from splitting	35
Accessing e-mail servers with System i Navigator	13	Receiving delivery status of e-mail	35
Configuring TCP/IP for e-mail	14	Hosting a Domino and SMTP server on the same	
Configuring Simple Mail Transfer Protocol and		system	36
Post Office Protocol servers for e-mail	15	Hosting Domino LDAP and Directory Server on	
Configuring the Simple Mail Transfer Protocol		the same system.	36
server	15	Managing Simple Mail Transfer Protocol server	
Enabling SSL between the SMTP server and		performance	37
client on the receiver system.	16	Changing values for the Simple Mail Transfer	
Enabling SSL between the SMTP server and		Protocol server	38
client on the sender system	16	Changing values for the Simple Mail Transfer	
Installing the receiver certificate authority		Protocol client	38
on the sender system	17	Selecting a new subsystem for Simple Mail	
Configuring the Post Office Protocol server.	17	Transfer Protocol server jobs.	38
Associating a certificate with the Post		E-mail reference information.	39
Office Protocol server	18	Mail server journal entries	39
Enrolling e-mail users	18	Simple Mail Transfer Protocol	43
Starting and stopping e-mail servers	19	Post Office Protocol.	44
Starting the e-mail servers	19	Troubleshooting e-mail	45
Stopping the e-mail servers	20	Determining problems with e-mail	45
Configuring a dial-up mail connection profile	20	Checking component journals	47
Configuring the ISP Dial-up Connection wizard	21	Tracking undelivered e-mail	47
Scheduling batch ISP e-mail jobs	21	Solving problems with the QtmmSendMail API	48
Configuring the SMTP server for dial-up mail		Checking the API call	48
retrieval	22	Checking the Multipurpose Internet Mail	
Supporting multiple domains	22	Extension file.	48
Securing e-mail	23	Checking mail server framework jobs.	49

Related information for E-mail	49	Programming interface information	52
Appendix. Notices	51	Trademarks	53
		Terms and conditions	53

E-mail

Use this information to plan for, configure, use, manage, and troubleshoot e-mail on your system.

This information assumes that you have worked on the i5/OS® operating system before and have a working knowledge of TCP/IP, Simple Mail Transfer Protocol (SMTP), and e-mail concepts.

What's new for V6R1

Read about new or significantly changed information for the E-mail topic collection in V6R1.

SMTP S/MIME support

The secure/Multipurpose Internet Mail Extensions (S/MIME) protocol can be used to verify e-mail senders when multiple transactions are in a Simple Mail Transfer Protocol (SMTP) delivery. Using the protocol, the e-mail document can be signed or encrypted. A new API QtmsCreateSendEmail provides the S/MIME support.

Read the following topics for a definition of S/MIME and for the configuration steps of using the new API in a scenario:

- “E-mail concepts” on page 2
- “Scenario: Configuring the QtmsCreateSendEmail API to use S/MIME” on page 6

SMTP authentication and SSL/TLS support

With SMTP authentication, you can now track an e-mail originator. The i5/OS SMTP server also supports sessions that are either protected by Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

- “Controlling Simple Mail Transfer Protocol access” on page 10
- “Tracking the e-mail sender” on page 24



POP SSL/TLS support

The i5/OS Post Office Protocol (POP) server now supports SSL/TLS sessions. The server can encrypt user IDs and passwords.

- “Setting up Post Office Protocol e-mail clients” on page 29

How to see what's new or changed

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

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

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what's new or changed this release, see the Memo to users.

PDF file for E-mail

You can view and print a PDF file of this information.


To view or download the PDF version of this document, select E-mail (about 692 KB).

Saving PDF files

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

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe® Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Related reference

“Related information for E-mail” on page 49

Product manuals, IBM® Redbooks® publications, Web sites, and other information center topic collections contain information that relates to the E-mail topic collection. You can view or print any of the PDF files.

E-mail concepts

You depend on electronic mail (e-mail) as an essential business tool. The i5/OS operating system uses protocols, like Simple Message Transfer Protocol (SMTP) and Post Office Protocol (POP), to make your e-mail run smoothly and efficiently on the network.

Distribution methods

These additional e-mail concepts discuss other e-mail distribution methods:

- Multipurpose Internet Mail Extensions (MIME)

MIME is a standardized method for organizing divergent file formats. SMTP is limited to 7-bit ASCII text with a maximum line length of 1000 characters. MIME was developed to support more advanced file types, such as rich text, images, and audio or video files. MIME encodes files of binary type data to appear as simple SMTP data, using headers to distinguish different file types within the message, before sending the message with SMTP. The mail client then receives the message and decodes it to the proper file types by interpreting the MIME headers to read the file.

- S/MIME

Secure/MIME is a secure version of the MIME protocol that allows users to send encrypted and electronically signed mail messages, even if users have different mail programs.

- AnyMail/400 framework

All incoming mail from SMTP for local users (users with mail accounts on this system) is processed by the AnyMail/400 framework. The mail server framework is a mail distribution structure that allows the distribution of e-mail. The mail server framework calls exit programs or snap-ins to handle specific mail types.

- Systems Network Architecture distribution services (SNADS)

SNADS is an IBM asynchronous distribution service that defines a set of rules to receive, route, and send electronic mail in a network of systems. In this topic, SNADS refers to a user profile in which the **Preferred address** is set to **User ID/Address**. The preferred address tells the mail server framework what fields to use in the system distribution directory for the address.

Related concepts

“Sending and receiving e-mail” on page 28

Your system is a mail server and has e-mail users (SNADS, POP, or Lotus® users) enrolled on it. Your e-mail users can send, receive, and read e-mail using either a POP client or a SNADS client.

Related tasks

“Holding Systems Network Architecture Distribution Services queues” on page 12

You can hold Systems Network Architecture Distribution Services (SNADS) distribution queues, which the SMTP application uses to distribute e-mail. This will provide you with extra protection to limit distribution of e-mail.

Simple Mail Transfer Protocol on i5/OS

Simple Mail Transfer Protocol (SMTP) is the protocol that allows the operating system to send and receive e-mail.

SMTP is essentially the end-to-end delivery of mail from one mail server to another. There is a direct connection between an SMTP sender (the client) and the destination SMTP receiver (the server). The SMTP client keeps the mail at the sender until it transmits and copies it successfully to the SMTP receiver (server).

SMTP on this operating system supports the distribution of notes, messages, and ASCII text documents. SMTP can support formats other than plain text by using the Multipurpose Internet Mail Extensions (MIME) protocol. MIME is the Internet standard for sending mail with headers that describe the contents of the mail messages to the receiving client. These messages can contain video, audio, or binary parts.

About SMTP e-mail delivery

In order for e-mail to reach its destination, SMTP must be able to deliver it to both the correct host and user ID that resides on that host. Suppose that mail is sent to bobsmith@mycompany.com.

First, SMTP checks to see if the e-mail addressee (bobsmith) is a user on the local server. If SMTP determines that it is not, SMTP forwards the e-mail to the next host server. The next host might or might not be the final host. SMTP determines the name of the host from addressing information that is found in the SMTP protocol.

SMTP then resolves the host's address by using either the Domain Name System (DNS) server or the local host table. The host name is what people use as a part of their e-mail account (mycompany.com); the IP address is what SMTP uses to find the correct mail server to send mail to (192.1.1.10).

1. The IPv6 addresses are ignored when the SMTP server looks up the host name addresses in the local host table.
2. If any DNS servers that are configured have IPv6 addresses, then all DNS servers configured must support recursion to resolve e-mail domains for which the configured servers are not an authority.

These topics relate DNS to SMTP:

- Domain Name System domain setup
- Mail and Mail Exchanger (MX) records

For inbound e-mail, the SMTP server first converts the destination host name into an Internet Protocol (IP) address. Because of the aliasing function, the server can have several host names. Therefore, the SMTP server uses the sockets interface to determine if the IP address is one of those used by the interfaces for the local host.

Related concepts

DNS

Mail and Mail Exchanger records

Related tasks

Domain Name System domain setup

“Configuring e-mail” on page 13

To set up e-mail on your system, you need to configure TCP/IP, set up Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers, and start the e-mail servers.

Post Office Protocol on i5/OS

The Post Office Protocol (POP) server is the i5/OS implementation of the Post Office Protocol Version 3 mail interface.

The POP server provides electronic mailboxes on this operating system from which clients can retrieve mail. Any mail client that supports the POP3 protocol can use this server, such as Netscape Mail, Outlook Express, or Eudora. Clients might be running on any platform, such as Windows®, Linux®, AIX®, or Macintosh.

The POP server serves as a temporary holding area for mail until it is retrieved by the mail client. When the mail client connects to the server, it queries the contents of its mailbox to see if there is any mail to retrieve. If there is, it retrieves one mail message at a time. After a message has been retrieved, the client instructs the server to mark that message for deletion when the client session is complete. The client retrieves all of the messages in the mailbox and then issues a command that tells the server to delete all of the messages that are marked for deletion and to disconnect from the client.

POP mail clients use *verbs* to communicate with the POP server. Verbs supported by the POP server for this operating system are described in the Post Office Protocol topic.

Related tasks

“Accessing e-mail servers with System i Navigator” on page 13

You can use System i™ Navigator to configure and manage Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) e-mail servers.

“Configuring Simple Mail Transfer Protocol and Post Office Protocol servers for e-mail” on page 15
To use e-mail, you need to configure Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers on your system.

Related reference

“Post Office Protocol” on page 44

The Post Office Protocol (POP) Version 3 mail interface is defined in Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), and RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC is the mechanism used to define evolving Internet standards.

Related information



RFC Index

Scenarios: E-mail

- | These scenarios illustrate how e-mail is processed between local users and how you can configure the QtmsCreateSendEmail API to use S/MIME.

Scenario: Sending and receiving e-mail locally

This scenario demonstrates how e-mail is processed between local users.

Situation

Jane Smith, the Human Resources director, needs to send a message to Sam Jones in the Legal department. They both work at MyCompany headquarters. By following this process, you can see how e-mail is handled on the system.

The objectives of this example are as follows:

- Demonstrate how e-mail clients and servers relate to each other, and how a message is processed
- Use the SMTP server to send mail
- Deliver mail to a POP user

Details

Jane is using the Netscape mail client. She writes a message and sends it to SamJones@mycompany.com. The following figure illustrates the path that the mail message takes through the network.

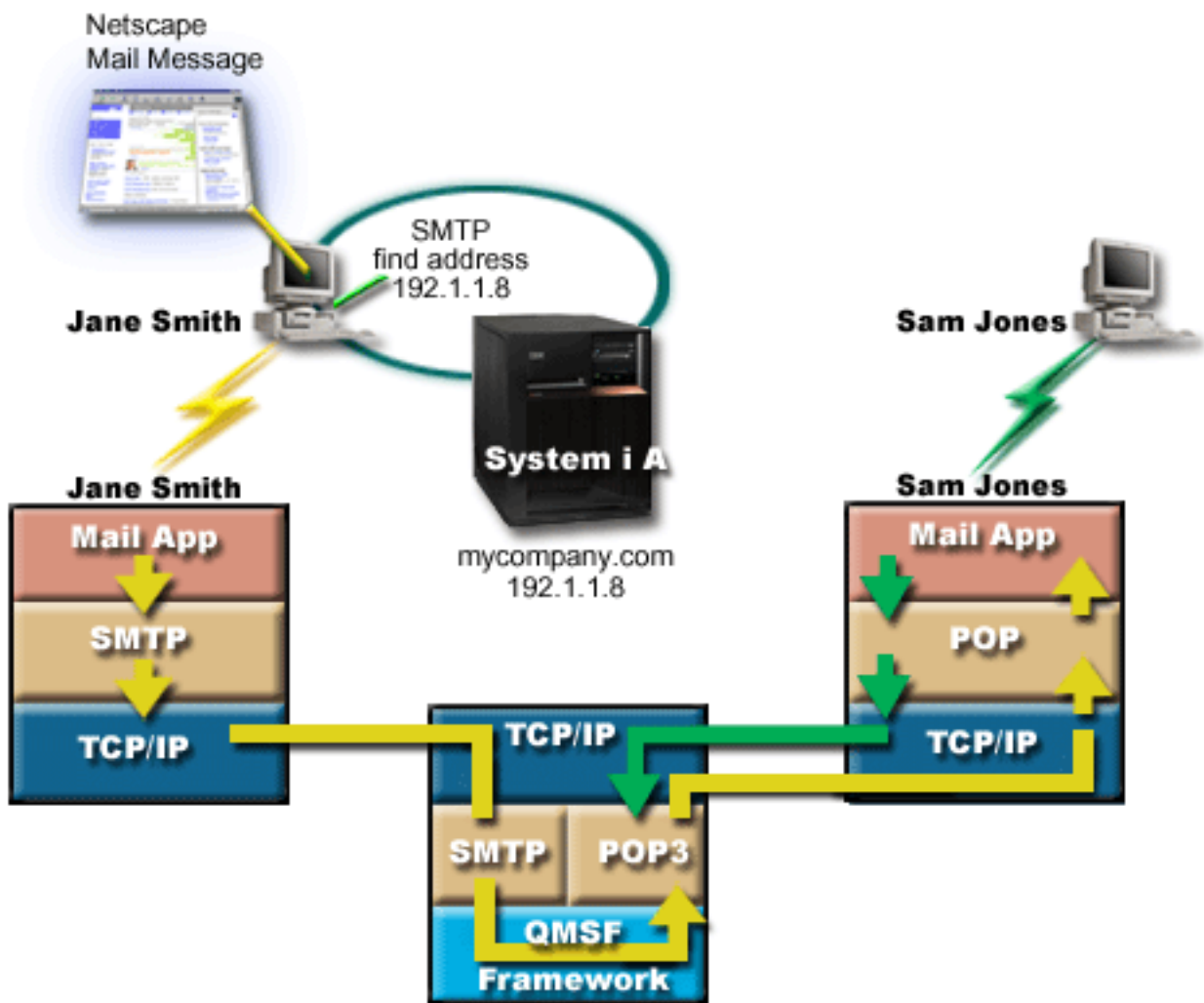


Figure 1. Sample network configuration

The following text describes each phase of the path the mail message takes through the network.

Phase 1: SMTP client to SMTP server

The SMTP client on Jane's PC uses the configuration data that was entered for the outgoing server and identity. The identity field is used for the **From** address. The outgoing server is the host that is contacted by the PC SMTP client. Because the address is entered as a domain, the SMTP client queries Domain Name System (DNS) to get the IP address of the SMTP server, and discovers that it is 192.1.1.8.

The SMTP client now contacts the SMTP server on the SMTP port (Port 25 at 192.1.1.8). The dialog that is used between the client and the server is the SMTP protocol. The SMTP server accepts the delivery of the mail, and the message is transmitted from the client to the server using TCP/IP.

Phase 2: SMTP server delivers the message to the POP server

The SMTP server tests the domain of the recipient to see if it is local. Because it is local, the mail is written out to an integrated file system file and the QMSF Framework Create Message application programming interface (API) is used to put the message information in the QMSF queue. The QMSF framework allows the distribution of e-mail, calling exit programs or snap-ins to handle specific mail types. The message information identifies Sam's address as SMTP format, so the framework calls the SMTP Address Resolution exit program. This program again checks that the message is local. Because it is local, it uses the system distribution directory (data entered through WRKDIR) to find the recipient's SMTP address. It finds Sam's address, and finds the mail service level is system message store in the directory entry for this user; therefore it recognizes it as a POP account. Then SMTP Address Resolution adds his profile information to the message information. It marks the information as POP local delivery. The QMSF Framework then calls the POP Local Delivery exit program, which finds the profile information and the name of the integrated file system file and delivers the mail to Sam's mailbox.

Phase 3: POP client retrieves message for Sam Jones from the POP server

Some time later, Sam decides to use his mail client (Netscape) to check his mailbox for e-mails. The POP client on his PC is configured to check the POP server at mycompany.com for the user name SamJones and password (*****). The domain name is again changed to an IP address (using DNS). The POP client contacts the POP server using the POP port and the POP3 protocol. The POP server on the operating system checks whether the mailbox user name and password match the profile and password of an i5/OS user. After it is validated, the profile name is used to find Sam's mailbox. The POP client loads the message, and sends a request back to the POP server to delete the mail from the POP mailbox. The message is then displayed in Netscape for Sam to read.

Related concepts

"Planning for e-mail" on page 9

Before setting up e-mail, you must have a basic plan for how to use e-mail on your system.

Related reference

"Simple Mail Transfer Protocol" on page 43

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending and receiving e-mail. It is typically used with POP3 or Internet Message Access Protocol to save messages in a server mailbox and download them periodically from the server for the user.

"Post Office Protocol" on page 44

The Post Office Protocol (POP) Version 3 mail interface is defined in Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), and RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC is the mechanism used to define evolving Internet standards.

| Scenario: Configuring the QtmsCreateSendEmail API to use S/MIME

| This scenario demonstrates how you can configure the QtmsCreateSendEmail API to use secure/MIME (S/MIME).

| Situation

| The user John Smith whose user ID is jsmith wants to configure the QtmsCreateSendEmail API to use S/MIME. S/MIME is a more secure way to send e-mail programmatically than using the QtmmSendMail API.

Details

To send signed and encrypted e-mails, John needs to have the following options installed on his system that runs i5/OS V6R1:

- i5/OS PASE (5761-SS1 option 33)
- Digital Certificate Manager (5761-SS1 option 34)
- OpenSSL (5733-SC1 option 1)

Creating a user certificate store

Using S/MIME requires a repository of the user certificates, which is called the user certificate store. On the operating system, users' certificates use the naming convention *userid.usrcrt*. The certificates are in the /qibm/userdata/icss/cert/download/client directory.

John must set up the user certificate store for his own user profile under which the job of creating and sending mail messages is run. He can use the Digital Certificate Manager (DCM) to manage the user certificate store.

To create a user certificate store, complete the following steps:

1. Create a subdirectory using the name of the user profile:

```
cd /qibm/userdata/icss/cert/download/client
mkdir jsmith
```

2. Using your Web browser, go to the System i Tasks page on your system at http://your_system_name:2001.

3. Select **Digital Certificate Manager** from the list of products on the System i Tasks page to access the DCM user interface. Click **Create New Certificate Store** in the left pane.

4. On the Create New Certificate Store page, select **Other System Certificate Store** and click **Continue**.

5. On the Create a Certificate in New Certificate Store page, select **No - Do not create a certificate in the certificate store**.

6. On the Certificate Store Name and Password page, set the certificate store path name and the password. Set your certificate store path to include your user ID. For instance, John sets his store path as /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.

Exporting the sender's user certificate to System i

John's Web browser is Internet Explorer (IE) 6. The sender's user certificate is obtained from the Certificate Authority (CA) and installed on IE 6.

To export the sender's user certificate to the System i platform, John performs the following steps:

1. In the IE window, select **Tools** → **Internet Options**.
2. On the **Content** tab, click **Certificates**.
3. On the **Personal** tab, select the sender certificate and click **Export**.
4. On the Welcome to the Certificate Export Wizard page, click **Next**.
5. On the Export Private Key page, select **Yes, export the private key** and click **Next**.
6. For the Export File Format page, select **Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)** under **Personal Information Exchange - PKCS #12 (.PFX)**.
7. On the Password page, enter the password for the certificate.
8. On the File to Export page, specify the name of the file you want to export, for instance, C:\temp\jsmithcert.pfx, and click **Next**.
9. On the Completing the Certificate Export Wizard page, click **Finish**.

- | 10. Send the sender user certificate jsmithcert.pfx in ASCII mode, using FTP, to the System i platform. In this example, it is assumed that the file is sent to the System i integrated file system directory /home/jsmith. For details about how to import this certificate, refer to “Importing the sender certificate to System i.”

| Exporting the recipient's user certificates to System i

| To export the sender recipient's certificate to the System i platform, John completes the following steps:

- | 1. In the IE window, select **Tools** → **Internet Options**.
- | 2. Click the **Content** tab on the Internet Options page, and then click **Certificates**.
- | 3. On the **Personal** tab on the Internet Options page, select the certificate, and click **Export**.
| If more than one certificate exists, you need to repeat steps 3 through 7 for all the certificates.
- | 4. On the Welcome to the Certificate Export Wizard page, click **Next**.
- | 5. On the Export File Format page, select **DER encoded binary X.509 (.CER)**.
- | 6. On the File to Export page, specify the name of the file you want to export, for instance, C:\temp\receiveruser.cer, and click **Next**.
- | 7. On the Completing the Certificate Export Wizard page, click **Finish**.
- | 8. Send the recipient's user certificate receiver.cer in ASCII mode, using FTP, to the System i platform. In this example, it is assumed that the file is sent to the System i integrated file system directory /home/jsmith. For details about how to import the recipient certificate, refer to “Importing the recipient certificate to System i.”
- | 9. Repeat all the preceding steps for each recipient that is used in S/MIME.

| Importing the sender certificate to System i

| Then John needs to import his user certificate and private key into the user certificate store using DCM. The password for the imported certificate must be the same as that of the keystore. He also needs to import all the certificates of the users to whom he wants to send e-mail.

- | 1. Using your Web browser, go to the System i Tasks page on your system at http://your_system_name:2001.
- | 2. Select **Digital Certificate Manager** from the list of products on the System i Tasks page to access the DCM user interface.
- | 3. On the Select a Certificate Store page, select **Other System Certificate Store** and click **Continue**.
- | 4. On the Certificate Store Name and Password page, enter your certificate store path and file name and the password, and click **Continue**. For John, the file name is /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
- | 5. Expand **Manage Certificates** → **Import Certificate**. Select **Server or client** to import the sender certificate. Click **Continue**.
- | 6. On the Import Server or Client Certificate page, enter the integrated file system directory and file name of the sender certificate and click **Continue**. In “Exporting the sender's user certificate to System i” on page 7, the integrated file system directory and file is /home/jsmith/ jsmithcert.pfx.
- | 7. Specify the certificate label, that is, the e-mail address of the sender in lowercase. Click **Continue**.
- | 8. Click **OK**.

| Importing the recipient certificate to System i

| To import the recipient certificate to the System i platform, follow these steps:

- | 1. Using your Web browser, go to the System i Tasks page on your system at http://your_system_name:2001.

- | 2. Select **Digital Certificate Manager** from the list of products on the System i Tasks page to access the DCM user interface.
 - | 3. On the Select a Certificate Store page, select **Other System Certificate Store** and click **Continue**.
 - | 4. On the Certificate Store Name and Password page, enter your certificate store path and file name and the password, and click **Continue**. For John, the file name is /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
 - | 5. Expand **Manage Certificates** → **Import Certificate**. Select **Certificate Authority (CA)** to import the recipient certificate. Click **Continue**.
 - | 6. On the Import Certificate Authority (CA) Certificate page, enter the integrated file system directory and file name of the recipient certificate and click **Continue**. In “Exporting the recipient’s user certificates to System i” on page 8, the integrated file system directory and file for the recipient is /home/jsmith/receiveruser.cer.
 - | 7. Specify the CA certificate label, that is, the e-mail address of the recipient in lowercase. Click **Continue**.
 - | 8. Repeat all the preceding steps for each recipient certificate that the sender needs to use.
- | **Related concepts**
- | Digital Certificate Manager
- | **Related reference**
- | Create and Send MIME E-mail (QtmsCreateSendEmail) API

Planning for e-mail

Before setting up e-mail, you must have a basic plan for how to use e-mail on your system.

Before you start setting up e-mail, answer the following questions:

1. What will my e-mail addresses look like?
2. What is the IP address of my Domain Name Server (DNS)?
3. Do I have a firewall? If the answer is yes, what is its IP address?
4. Do I have a mail proxy, mail router, or mail relay? If the answer is yes, what is its IP address?
5. Will I be using a Domino® database?
6. Will I be using the i5/OS POP server to receive mail?

You might want to refer to the e-mail scenario for basic information about how e-mail works.

If you will be using the Domino server and the i5/OS SMTP server, refer to Hosting a Domino and SMTP server on the same system topic. For additional information about Domino, refer to the Domino topic or the Lotus Domino for i5/OS Web site.

If you do not plan to use the SMTP or POP servers, disable them to ensure that they will not be used without your knowledge.

Related concepts

“Scenario: Sending and receiving e-mail locally” on page 4

This scenario demonstrates how e-mail is processed between local users.

Domino

Related tasks

“Configuring e-mail” on page 13

To set up e-mail on your system, you need to configure TCP/IP, set up Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers, and start the e-mail servers.

“Hosting a Domino and SMTP server on the same system” on page 36

If you are running Domino and Simple Mail Transfer Protocol (SMTP) on the same system, it is suggested that you configure each one to bind to a specific IP address.

Related information

 Lotus Domino for i5/OS

Controlling e-mail access

You need to control who accesses your system through e-mail to protect your data from malicious attacks.

This section provides tips for protecting your e-mail servers from flooding and spamming.

Related concepts

Independent disk pool examples

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Related tasks

“Restricting the relay of messages” on page 25

To prevent people from using your e-mail server for spamming or sending large amounts of bulk e-mail, you can use the relay restriction function to specify who can use your system for relaying messages. However, you cannot authenticate your e-mail when you restrict relaying messages.

“Restricting connections” on page 27

To ensure the security of your system, you need to prevent the connection of users who might abuse your e-mail server.

Related information

 AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet

Controlling Simple Mail Transfer Protocol access

To prevent your system from being attacked by malicious or unsolicited mail (spam), you must control Simple Mail Transfer Protocol (SMTP) access.

If you want to allow SMTP clients to access your system, you need to protect your system from attack by doing the following tasks:

- If possible, avoid using an *ANY *ANY entry in the system distribution directory. When your system does not have an *ANY *ANY entry, it is more difficult for someone to attempt to use SMTP to overwhelm your system or your network. When your auxiliary storage is filled with unwanted mail that is being routed through your system to another system, your system or your network is overwhelmed.
 - Set adequate threshold limits for your auxiliary storage pools (ASPs) to prevent a user from overwhelming your system with unwanted objects. You can display and set the thresholds for ASPs by using either system service tools (SSTs) or dedicated service tools (DSTs).
 - Tune the maximum number of prestart jobs that can be created by using the Change Prestart Job Entry (CHGPJE) command. This limits the number of jobs created during a denial of service attack. The default is 256 for the maximum threshold.
 - Prevent outsiders from using your connection to send unsolicited e-mail (spam) by restricting relays and connections.
- | • On systems running i5/OS V6R1, you can prevent spam by requiring authentication to send e-mail. If
| a remote server requires authentication, you can set up authentication on your local server.

Related reference

- | Change SMTP Attributes (CHGSMTPA) command

Controlling Post Office Protocol access

To ensure the security of your system, you need to control Post Office Protocol (POP) access.

- | You can specify whether the POP server uses encryption to secure POP datastreams including user IDs
- | and passwords. The encryption is provided with the Secure Sockets Layer (SSL) or the Transport Layer
- | Security (TLS). To indicate whether secure POP sessions are supported, set the ALWSSL parameter on the
- | Change POP Server Attributes (CHGPOPA) CL command.

If you want to allow POP clients to access your system, be aware of the following security considerations:

- | • The POP mail server provides authentication for clients who attempt to access their mailboxes. The
- | client sends a user ID and password to the server.

The POP mail server verifies the user ID and password against the i5/OS user profile and password for that user. Because you do not have control over how the user ID and password are stored on the POP client, you might want to create a special user profile that has limited authority on your system. To prevent anyone from using the user profile for an interactive session, you can set the following values in the user profile:

Set initial menu (INLMNU) to *SIGNOFF

Set initial program (INLPGM) to *NONE

Set limit capabilities (LMTCPB) to *YES

- To prevent a malicious intruder from overwhelming your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). The ASP storage threshold prevents your system from stopping because the operating system does not have sufficient working space. You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST).
- Although you need to ensure that your ASP threshold prevents your system from being flooded, you also need to ensure that your system has adequate space to properly store and deliver mail. If your mail server cannot deliver mail because the system does not have adequate storage for transient mail, this is an integrity problem for your users. When system storage use is high, mail stops running. Typically, storage space is not a significant problem. When a client receives mail, the mail server deletes the mail from the system.

Related concepts

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Preventing e-mail access

Depending on how you use your system, you might want to prevent users from accessing e-mail through SMTP and POP servers. You can prevent e-mail access entirely or allow access occasionally.

Preventing Simple Mail Transfer Protocol access

If you do not want anyone to use Simple Mail Transfer Protocol (SMTP) to distribute mail to or from your system, you should prevent the SMTP server from running.

SMTP is configured by default to start automatically when TCP/IP starts. If you do not plan to use SMTP at all, do not configure it on your system (or allow anyone else to configure it).

Preventing Simple Mail Transfer Protocol from starting when TCP/IP starts:

You might need to use Simple Mail Transfer Protocol (SMTP) occasionally, but want to limit the amount of access users have to the SMTP server.

To prevent SMTP server jobs from starting automatically when you start TCP/IP, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.

3. Clear **Start when TCP/IP starts**.

Preventing access to Simple Mail Transfer Protocol ports:

To secure your Simple Mail Transfer Protocol (SMTP) server from unknown applications, you might want to prevent access to SMTP ports.

To prevent access to SMTP from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for SMTP, complete the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **TCP/IP Configuration** and select **Properties**.
3. In the TCP/IP Configuration Properties window, click the **Port Restrictions** tab.
4. On the Port Restrictions page, click **Add**.
5. On the Add Port Restriction page, specify the following settings:
 - **User name:** Specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.
 - **Starting port:** 25
 - **Ending port:** 25
 - **Protocol:** TCP
6. Click **OK** to add the restriction.
7. On the **Port Restrictions** page, click **Add** and repeat the procedure for UDP.
8. Click **OK** to save your port restrictions and close the **TCP/IP Configuration Properties** window. The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

Holding Systems Network Architecture Distribution Services queues:

You can hold Systems Network Architecture Distribution Services (SNADS) distribution queues, which the SMTP application uses to distribute e-mail. This will provide you with extra protection to limit distribution of e-mail.

To hold the distribution queues, enter the following commands on the character-based interface:

```
HLDDSTQ DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ DSTQ(QSMTPQ)PTY(*HIGH)
```

Related concepts

“E-mail concepts” on page 2

You depend on electronic mail (e-mail) as an essential business tool. The i5/OS operating system uses protocols, like Simple Message Transfer Protocol (SMTP) and Post Office Protocol (POP), to make your e-mail run smoothly and efficiently on the network.

Preventing Post Office Protocol access

If you do not want anyone to use Post Office Protocol (POP) to access your system, you should prevent the POP server from running.

If you do not plan to use POP at all, do not configure it on your system (or allow anyone else to configure it).

Preventing Post Office Protocol from starting when TCP/IP starts:

You might need to use Post Office Protocol (POP) occasionally, but want to limit the amount of access users have to the POP server.

The POP server is configured by default to start automatically when TCP/IP starts. To prevent POP server jobs from starting automatically when you start TCP/IP, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **POP** and select **Properties**.
3. Clear **Start when TCP/IP starts**.

Preventing access to Post Office Protocol ports:

To secure your Post Office Protocol (POP) server from unknown applications, you might want to prevent access to POP ports.

To prevent the POP server from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for POP, complete the following steps:

1. In System i Navigator, connect to your system, and expand **Network** → **Servers** → **TCP/IP**.
2. Right-click **TCP/IP Configuration** and select **Properties**.
3. In the TCP/IP Configuration Properties window, click the **Port Restrictions** tab.
4. On the Port Restrictions page, click **Add**.
5. On the Add Port Restriction page, specify the following settings:
 - **User name:** Specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.
 - **Starting port:** 110 995
 - **Ending port:** 110 995
 - **Protocol:** TCP
6. Click **OK** to add the restriction.
7. On the Port Restrictions page, click **Add** and repeat the procedure for UDP.
8. Click **OK** to save your port restrictions and close the TCP/IP Configuration Properties window.

The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

Configuring e-mail

To set up e-mail on your system, you need to configure TCP/IP, set up Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers, and start the e-mail servers.

Related concepts

“Simple Mail Transfer Protocol on i5/OS” on page 3

Simple Mail Transfer Protocol (SMTP) is the protocol that allows the operating system to send and receive e-mail.

“Planning for e-mail” on page 9

Before setting up e-mail, you must have a basic plan for how to use e-mail on your system.

Accessing e-mail servers with System i Navigator

You can use System i Navigator to configure and manage Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) e-mail servers.

To access POP or SMTP in System i Navigator, follow these steps:

1. Double-click the **Client Access Express** folder.
2. Double-click **System i Navigator**. If this is your first time using System i Navigator, click the **New Connection** icon to establish a connection to your system.
3. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
4. Double-click **SMTP** to open the SMTP Properties dialog, or double-click **POP** to open the POP Properties dialog.

Related concepts

“Post Office Protocol on i5/OS” on page 4

The Post Office Protocol (POP) server is the i5/OS implementation of the Post Office Protocol Version 3 mail interface.

Configuring TCP/IP for e-mail

You need to set up TCP/IP before you can configure e-mail on your system.

If you are setting up e-mail on your system for the first time, complete the following steps. If you already have TCP/IP configured on your system, you can proceed directly to Configuring Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers for e-mail.

1. In System i Navigator, expand *your system* → **Network** → **TCP/IP Configuration**.
2. Right-click **Interfaces** and select **New Interface** and the type of network the new interface represents. Follow the wizard’s instructions to create a new TCP/IP interface. The wizard asks you to supply the following information:

- Type of connection
- Hardware resource
- Line description
- IP address
- Host name
- Domain name

The host name and domain name you use for the wizard constitute your fully qualified domain name. SMTP requires a fully qualified domain name to communicate with other SMTP hosts.

For example, if the local host name is ASHOST and the local domain name is DOMAIN.COMPANY.COM, the fully qualified domain name is ASHOST.DOMAIN.COMPANY.COM.

- Servers to start
3. After you are finished with the wizard, right-click **TCP/IP** and select **Properties**. The TCP/IP Properties dialog appears.
 4. Click the **Host Table** tab.
 5. Click **Add**. The TCP/IP Host Table Entry dialog appears.
 6. Enter the IP address and the host name you used in the New TCP/IP Interface wizard.
 7. Click **OK** to close the TCP/IP Host Table Entry dialog.
 8. Click **OK** to close the TCP/IP Properties dialog.

Related concepts

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Related tasks

“Configuring Simple Mail Transfer Protocol and Post Office Protocol servers for e-mail” on page 15
To use e-mail, you need to configure Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers on your system.

Configuring Simple Mail Transfer Protocol and Post Office Protocol servers for e-mail

To use e-mail, you need to configure Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) servers on your system.

Note: Both the SMTP and the POP server must be correctly configured.

Related concepts

“Post Office Protocol on i5/OS” on page 4

The Post Office Protocol (POP) server is the i5/OS implementation of the Post Office Protocol Version 3 mail interface.

Related tasks

“Configuring TCP/IP for e-mail” on page 14

You need to set up TCP/IP before you can configure e-mail on your system.

Configuring the Simple Mail Transfer Protocol server

When you configured TCP/IP, the system automatically configured SMTP for you. However, you still need to change a few SMTP properties to ensure that the SMTP server works correctly for e-mail.

To change the SMTP properties, perform the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the tabs listed in the following table to set the field values indicated in the Then perform the following action column.

Click this tab	Then perform the following action
General	Select Start when TCP/IP is started . ¹
General	Select No maximum for the Message split size field.
General	If you have a mail router, enter the name of the mail router, for example, mailrouter.company.com. The mail router name is the system name, where SMTP routes the mail if the e-mail is not local mail. See the System i Navigator help for more details.
General	If you have a firewall set up, select Forward outgoing mail to router through firewall .
General	If you exchange e-mail with Domino servers, clear the Interpret percent sign as routing character field.
General	If you want to forward all nonlocal e-mail to another SMTP server, specify the fully qualified mail exchanger domain name in the Forwarding mailhub domain field.
General	If you want the SMTP server to support bare line feed (LF) or carriage return-line feed (CRLF), select Allow bare line feed . If you want the SMTP server to support CRLF only, clear the Allow bare line feed check box.
Automatic Registration	If you are using the SNDDST command to send e-mail and the RCVDST command to receive e-mail, and you are using SNADS addressing instead of internet addressing, select the Automatically add remote users to system distribution directory check box.
Automatic Registration	If you are using the SNDDST command to send e-mail and the RCVDST command to receive e-mail, click System alias table in the Add users to field.
¹ This change takes effect the next time the SMTP server is started.	

4. Click **OK** to accept the changes.

Related tasks

“Authenticating e-mail for local and relay” on page 24

You can now prevent your server from spam by requiring authentication to send e-mail. You cannot require authentication if you want to restrict relaying messages. It is recommended that you set up authentication for your server.

| Enabling SSL between the SMTP server and client on the receiver system:

| To enable SSL between the SMTP server and client on the receiver system, complete these steps. It is assumed that a server certificate has been created on the SMTP server.

| To perform this task, make sure that you are connected to the receiver system.

| Starting and configuring DCM

- | 1. In your Web browser, connect to the SMTP server: `http://your_system: 2001/`
- | 2. On the i5/OS Tasks page, select **Digital Certificate Manager** and then click **Select a Certificate Store**.
- | 3. On the Select a Certificate Store page, select ***SYSTEM** and click **Continue**.
- | 4. On the Certificate Store and Password page, enter the password for your certificate store.
- | 5. Expand **Manage Applications** → **Update certificate assignment** and select **Server**.
- | 6. Select **i5/OS TCP/IP SMTP server** and click **Update Certificate Assignment** if needed.

| Configuring the SMTP server

| To enable SSL support, set the ALWAUTH parameter to either ***LCLRLY** or ***RELAY** using the Change SMTP Attributes (CHGSMTPA) command.

- | • If you set the parameter to ***RELAY**, only e-mails sent from the other SMTP server support the use of SSL.
- | • If you set the parameter to ***LCLRLY**, the Verify MSF messages (VFYMSFMSG) and Verify from user (VFYFROMUSR) parameters are also enabled. The default value can also result in the rejection of certain e-mails. Determine if you want the rejections support enabled.

| Configuring the SMTP client

| You must configure the System i SMTP client so that it can log on to the System i SMTP receiver server. Use the Add SMTP List Entry (ADDSMTPLE) CL command to add an entry to the host authentication list:

| `ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(yoursystem.realm.com) USERNAME(receiver) PASSWORD(xxxx)`

| The host name, which is stored in uppercase, must match the e-mail address. If the e-mail address is myemail@yoursystem, the following entry needs to be added:

| `ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(YOURSYSTEM) USERNAME(receiver) PASSWORD(xxxx)`

| Enabling SSL between the SMTP server and client on the sender system:

| You must be connected to the sender system to perform this task.

- | 1. In your Web browser, connect to the SMTP server: `http://your_system: 2001/`
- | 2. On the i5/OS Tasks page, select **Digital Certificate Manager** and then click **Select a Certificate Store**.
- | 3. On the Select a Certificate Store page, select ***SYSTEM** and click **Continue**.
- | 4. On the Certificate Store and Password page, enter the password for your certificate store and click **Continue**. If you do not have a User Certificate or want to create a User Certificate, complete steps 5 through 8 on page 17; otherwise, skip to step 9 on page 17.
- | 5. On the Create Certificate page, select **User certificate** and click **Continue**.

- | 6. On the Create User Certificate page, specify the required fields for the certificate information and click **Continue**.
- | 7. In the Potential Scripting Violation window, Click **Yes**.
- | 8. On the Create User Certificate page, click **OK**. The system will use the client user certificate.
- | 9. Expand **Manage Applications** → **Update certificate assignment**, select **Server or client certificate**.
- | 10. On the Update Certificate Assignment page, select **Client** and click **Continue**.
- | 11. Select **i5/OS TCP/IP Client** and click the **Update Certificate Assignment** button.

| **Installing the receiver certificate authority on the sender system:**

- | If the receiver digital certificate is issued by a certificate authority (CA) that is unknown to the sender system, install the digital certificate for the certificate authority on the sender system.

| **Exporting the local CA certificate and sending it to the sender system**

- | It is assumed that the certificate authority is local; however, you can use this procedure to export any CA certificate that is not known to the sender system.

- | To export the local CA certificate, follow these steps:

- | 1. Click **Select a Certificate Store** and select **Local Certificate Authority (CA)**. Click **Continue**.
- | 2. On the Certificate Store and Password page, enter the password.
- | 3. Expand **Manage Local CA** → **Export** and select **File - Export to a file**. Click **Continue**.
- | 4. On the Export Certificate page, enter the directory and file name location to store the CA certificate. If a directory does not already exist, use the mkdir command to create one.
- | 5. On the Export Certificate Successful page, click **OK**.
- | 6. Use FTP in ASCII mode to send the CA certificate from the receiver system to the sender system.

| **Installing the CA certificate on the sending system**

- | 1. On the Select a Certificate Store page, select ***SYSTEM** and click **Continue**.
- | 2. On the Certificate Store and Password page, enter your password and click **Continue**.
- | 3. Expand **Manage Certificates** → **Import certificates**, select **Certificate Authority (CA)** and click **Continue**.
- | 4. On the Import Certificate Authority (CA) Certificate page, enter the directory where the receiver CA certificate is stored. Click **Continue**.
- | 5. Assign a certificate label to your certificate and click **Continue**. The following message is displayed:
The certificate has been imported.
- | 6. Click **OK**.

Configuring the Post Office Protocol server

You need to configure the Post Office Protocol (POP) server before you use it to deliver mails to POP clients.

When requested by the POP client, the POP server delivers mail to a POP client from the user's mailbox. You must configure the POP server to completely prepare your system for e-mail.

To configure the POP server for a mail program, such as Netscape Mail or Eudora Pro, complete the following steps:

- 1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
- 2. Double-click **POP**.

3. Refer to the following table to set the field values.

Click this tab	Then perform the following action
General	Select Start when TCP/IP is started .
General	If you want to allow both TLS/SSL and nonsecure POP sessions, select Both secure and nonsecure for the field Socket layer support to be started with server .
Configuration	Select No maximum for the Message split size field.
Configuration	If POP clients are logging on through dialup lines and receiving large pieces of mail, increase the Inactivity timeout value .
Mappings	Select Use only when unsupported CCSID is indicated .

4. Click **OK** to accept the changes.

Associating a certificate with the Post Office Protocol server:

Complete this task if you did not assign a certificate to the Post Office Protocol (POP) server application during the creation of the local Certificate Authority (CA) or if you have configured your system to request a certificate from a public CA.

1. Start IBM Digital Certificate Manager. If you need to obtain or create certificates, or otherwise set up or change your certificate system, do so now. See Configuring DCM for information about setting up a certificate system.
2. Click **Select a Certificate Store**.
3. Select ***SYSTEM**. Click **Continue**.
4. Enter the appropriate password for the *SYSTEM certificate store. Click **Continue**.
5. When the left navigational menu reloads, expand **Manage Applications**.
6. Click **Update certificate assignment**.
7. Select **Server application**. Click **Continue**.
8. Select **i5/OS TCP/IP POP Server**.
9. Click **Update Certificate Assignment** to assign a certificate to this POP Server.
10. Select a certificate from the list to assign to the server.
11. Click **Assign New Certificate**.
12. When you finish setting up the certificates for the POP server, click **Done**.

Enrolling e-mail users

You need to create user profiles to enroll e-mail users.

User profiles are how the i5/OS operating system identifies an addressee or sender of e-mail. Any user you want as part of your e-mail system must have a user profile on the system.

By creating a user profile for each user, you enroll the users in the system distribution directory automatically. The system distribution directory is what Simple Mail Transfer Protocol (SMTP) uses to determine where to deliver local e-mail.

To create user profiles for Systems Network Architecture Distribution Services (SNADS) and Post Office Protocol (POP) e-mail users, complete the following steps:

1. In System i Navigator, expand *your system* → **Users and Groups**.
2. Right-click **All Users** and select **New User**.
3. Type a user name and password for the user.

Note: This password will be used by POP users to access their POP mailboxes.

4. Click the **Capabilities** button.
5. Click the **Privileges** tab. Ensure that the Privilege class is **User**.
6. Click **OK**.
7. Click the **Personal** button.
8. Click the **Mail** tab.
9. Choose the **Mail Service Level**.
 - If your user is a SNADS user, select **User index**.
 - If your user is a POP3 mail user, select **System mailbox**.
10. Choose the **Preferred Address type**.
 - If your user is a SNADS user, select **User ID and address**.
 - If your user is POP3 mail user, select **SMTP name**.
11. Verify that the required domain name is displayed for the SMTP e-mail domain. The default name is typically correct, but if you have multiple local domains you might need to change it.
12. Click **OK**. If you are enrolling a SNADS user, the enrollment is complete. If you are enrolling a POP user who will use the i5/OS POP server only to retrieve e-mail, continue to the next step.
13. Click the **Jobs** button.
14. Click the **Session Startup** tab.
15. For the **Initial Menu** field, select **Sign off**. With this setting, any attempt to sign on the system, other than to retrieve e-mail or change a password, automatically signs the user off.
16. Click **OK**.
17. Click **OK**.
18. Repeat these instructions until all of the e-mail users have user profiles.

Related concepts

“Sending and receiving e-mail” on page 28

Your system is a mail server and has e-mail users (SNADS, POP, or Lotus users) enrolled on it. Your e-mail users can send, receive, and read e-mail using either a POP client or a SNADS client.

Related tasks

“Sending e-mail using Systems Network Architecture distribution services” on page 31

You can send e-mail from your system using a Systems Network Architecture distribution services (SNADS) client program. The sender of the e-mail must be a local SNADS user.

Starting and stopping e-mail servers

Start the required servers to ensure that everything works properly and that all the configuration changes you made take place. Sometimes, it might be necessary for you to restart the servers. This can be done by stopping the servers, and then completing the steps to start the servers again.

Related tasks

“Checking e-mail servers” on page 34

One of the most common problems with e-mail is that the proper servers are not started. Before using your e-mail servers, you need to verify the status of e-mail servers and make sure that they are all running.

Starting the e-mail servers

You can start your servers and make your system an e-mail server with enrolled e-mail users.

To start the servers, follow these steps:

1. In System i Navigator, expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and select **Properties**. The TCP/IP Configuration Properties dialog opens.

- If the TCP/IP status is Started, click **OK** and continue to the next step.
 - If not, click **Cancel** to close the TCP/IP Configuration Properties dialog; then right-click **TCP/IP Configuration** and select **Start**. Click **OK** when finished.
3. Expand **Servers** → **TCP/IP**. If the SMTP and POP servers are not started, then follow these steps to start them:
 - a. Right-click **SMTP** and select **Start**.
 - b. Right-click **POP** and select **Start**.
 4. Open the character-based interface and type STRMSF to start the Mail Server Framework.
 5. If you are using SNADS, type STRSBS QSNADS to start the QSNADS subsystem.

You have started your servers and your system is now running an e-mail server with enrolled e-mail users.

Stopping the e-mail servers

You can use System i Navigator to stop the e-mail servers.

To stop the servers, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**. If the SMTP and POP servers are started, then follow these steps to stop them:
 - a. Right-click **SMTP** and select **Stop**.
 - b. Right-click **POP** and select **Stop**.
2. Open the character-based interface and type ENDMSF to end the Mail Server Framework.
3. If you are using SNADS, type ENDSBS QSNADS to end the QSNADS subsystem.

Configuring a dial-up mail connection profile

If you do not have AT&T Global Network support, you must first configure a mail connection profile.

To manually create a dial-up connection profile, complete the following steps:

Note: If you have AT&T Global Network support, you can skip to Configuring the ISP Dial-up Connection wizard.

1. In System i Navigator, expand *your system* → **Network** → **Remote Access Services**.
2. Right-click **Receiver Connection Profiles** and select **New Profile**.
3. Select **PPP** for the **Protocol type**.
4. Select **Switched line** for **Connection type**.
5. Expand **TCP/IP Configuration** and select **Connections**.
6. Expand **Servers** → **TCP/IP**.
7. Right-click **SMTP** and select **Properties**.
8. Click the **Scheduler** tab. Select the **Start scheduler when SMTP is started** check box, and specify the connection profile that you created.
9. Click the **ETRAN** page and select the **Support ETRAN (Dial-up mail retrieval)** check box. Click **Add** to specify the domain name for your ISP's outgoing server's address.
10. Enable the firewall and point to the outgoing Internet service provider's (ISP's) mail server.
11. Continue with the wizard to set up a new ISP dial-up connection.

Related tasks

"Configuring the ISP Dial-up Connection wizard" on page 21

You need to configure a dial-up connection profile before using the Simple Mail Transfer Protocol (SMTP) scheduler function to send large amounts of e-mail through an Internet service provider.

Configuring the ISP Dial-up Connection wizard

You need to configure a dial-up connection profile before using the Simple Mail Transfer Protocol (SMTP) scheduler function to send large amounts of e-mail through an Internet service provider.

You can use the Internet service provider (ISP) Dial-up Connection wizard to configure the ISP dial-up connection profile.

Prerequisites:

If you do not have AT&T Global Network support, see *Configuring a dial-up mail connection profile* for a preliminary step. The connection wizard provides you with the IP addresses of the mail servers (SMTP and POP), their assigned domain name, account name, and password.

To run the wizard and configure your SMTP scheduler, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Remote Access Services**.
2. Right-click **Originator Connection Profiles** and select **New AT&T Global Network Dial Connection**.
3. On the Welcome panel, click **Next** to get started.
4. On the **Application Type** panel, select **Mail exchange application** and click **Next**.
5. Continue with the wizard to set up a new AT&T Global Network dial connection.

When you have configured the dial-up connection, you are ready to schedule batch ISP e-mail jobs.

Related tasks

“Configuring a dial-up mail connection profile” on page 20

If you do not have AT&T Global Network support, you must first configure a mail connection profile.

“Scheduling batch ISP e-mail jobs”

To limit the time required to establish a connection, you can schedule mail dial-up jobs to connect to your Internet service provider (ISP) at regular intervals. Use the SMTP scheduler to set the time intervals that you want your system to connect to your ISP and send your company’s e-mail.

Scheduling batch ISP e-mail jobs

To limit the time required to establish a connection, you can schedule mail dial-up jobs to connect to your Internet service provider (ISP) at regular intervals. Use the SMTP scheduler to set the time intervals that you want your system to connect to your ISP and send your company’s e-mail.

Prerequisites:

Use the ISP Dial-up Connection wizard to configure the connection.

To set the SMTP scheduler to send your e-mail to an ISP, complete the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **Scheduler** tab.
4. Select the **Start scheduler when SMTP is started** check box.
5. Select the **Point-to-point connection profile** you configured with the AT&T Global Network Dialer Wizard, or select a manually configured **Point-to-point connection profile**.
6. Set the **Mail transfer interval** to the number of minutes you want SMTP to deliver your queued e-mail.
7. If your ISP is not with the AT&T Global Network, select the **Issue ETRN when connecting to remote server** check box.
8. Enter the Server IP address for the incoming mail server on the ISP’s network, and enter the Registered ISP host.domain for which this SMTP server will issue an ETRN.

9. Click **OK**.

Related tasks

“Configuring the ISP Dial-up Connection wizard” on page 21

You need to configure a dial-up connection profile before using the Simple Mail Transfer Protocol (SMTP) scheduler function to send large amounts of e-mail through an Internet service provider.

“Configuring the SMTP server for dial-up mail retrieval”

You can use the Simple Mail Transfer Protocol (SMTP) server to receive mail for remote dial-up branch offices.

Configuring the SMTP server for dial-up mail retrieval

You can use the Simple Mail Transfer Protocol (SMTP) server to receive mail for remote dial-up branch offices.

The system must have a fixed IP address and be registered with a DNS. Each host.domain for which the remote dial-up servers will be retrieving mail must also have MX entries in the DNS pointing to this system. The system must also have aliases for these host.domains in its local host table. If the remote dial-up servers are running on the i5/OS operating system, then they must be configured for scheduled batch ISP e-mail jobs.

To receive e-mail requests from remote dial-up mail servers, complete the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **ETRN** tab.
4. Select the **Support ETRN (Dial-up mail retrieval)** check box.
5. Click **Add** to specify your ISP's host and domain name. This can be done multiple times if multiple mail servers are requesting their mail.
6. Click **OK**.

Related tasks

“Scheduling batch ISP e-mail jobs” on page 21

To limit the time required to establish a connection, you can schedule mail dial-up jobs to connect to your Internet service provider (ISP) at regular intervals. Use the SMTP scheduler to set the time intervals that you want your system to connect to your ISP and send your company's e-mail.

Supporting multiple domains

You can configure your Simple Mail Transfer Protocol (SMTP) server to support multiple domains in order to host Internet Service Provider (ISP) functions.

For the SMTP server to host ISP functions, it is necessary for SMTP to appear to operate in multiple domains. The SMTP client uses this configuration information to know which interface to bind to when it sends the e-mail, and which mail to consider local (that is, to resolve and send on its own) or to forward to a configured firewall mail daemon.

1. In System i Navigator, expand *your system* → **TCP/IP** → **Network**.
2. Right-click **SMTP** and select **Properties**.
3. Click the **Multiple Domains** tab.
4. Click **Add** to specify the domains and interfaces that you would like to support.
5. Click **OK**.

Related concepts

“Prerequisites for an e-mail router” on page 23

This topic tells what you should do before you configure an e-mail router.

Securing e-mail

You can use firewalls, restrict relays and connections, and filter out viruses to help secure e-mail.

It is important to promote a secure environment in your Simple Mail Transfer Protocol (SMTP) server. You must protect your SMTP server and your users from internal and external hindrances.

Related concepts

“E-mail concepts” on page 2

You depend on electronic mail (e-mail) as an essential business tool. The i5/OS operating system uses protocols, like Simple Message Transfer Protocol (SMTP) and Post Office Protocol (POP), to make your e-mail run smoothly and efficiently on the network.

Related reference

Create and Send MIME E-mail (QtmsCreateSendEmail) API

Related information

E-mail security

Sending e-mail through a router or firewall

An e-mail router is an intermediate system that Simple Message Transfer Protocol (SMTP) delivers mail to when it cannot locate the recipient’s exact IP address.

The e-mail router routes the e-mail to the IP address or to another router. Route your outgoing e-mail to an alternative system if your local server fails to deliver the e-mail to the system. If you have a firewall, you can use the firewall as your router.

Before you follow these steps to configure a router, see the “Prerequisites for an e-mail router.”

To set the router, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **General** tab.
4. Enter the Mail router name.

To route e-mail through a firewall, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **General** tab.
4. Enter the name of the firewall; for example, FWAS400.company.com in the **Mail Router** field.
5. Select **Forward outgoing mail to router through firewall**.

Prerequisites for an e-mail router

This topic tells what you should do before you configure an e-mail router.

Before you configure an e-mail router, consider the following aspects:

- The intermediate server does not have to be an i5/OS operating system. The mail router only requires a host table that contains all host servers to which it needs to route e-mail. If an i5/OS operating system is the mail router, it does not require any particular system level.
- You can set up only one intermediate server for routing between the source and target server. You cannot nest mail routers.
- Simple Mail Transfer Protocol (SMTP) must be able to get an IP address for the mail router when it starts, either from the local host table or through the Domain Name System (DNS) server. If SMTP cannot get an IP address for the mail router, then SMTP runs without using a router.

- The SMTP client firewall support uses the mail router to forward e-mail that is destined for a host outside the local (protected) domain. In order to deliver e-mail, the mail router must be a server that is authorized to forward e-mail through the firewall. Also, mail recipients whose domain is not on the i5/OS operating system go through the router when you turn on the SMTP firewall support. i5/OS V5R1 and later supports multiple local domains. You can configure multiple domains that do not send mail through the firewall.

Related tasks

“Supporting multiple domains” on page 22

You can configure your Simple Mail Transfer Protocol (SMTP) server to support multiple domains in order to host Internet Service Provider (ISP) functions.

Authenticating e-mail for local and relay

You can now prevent your server from spam by requiring authentication to send e-mail. You cannot require authentication if you want to restrict relaying messages. It is recommended that you set up authentication for your server.

To enable authentication for your server, complete these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **Authentication** tab and set the field values indicated in the Then perform the following action column.

Click this tab	Then perform the following action
Authentication	If you want the server to use TLS/SSL to authenticate it locally and when relaying the messages, select Require TLS/SSL and authenticate it locally and when using the relay .
Authentication	If you want the server to use TLS/SSL to authenticate it only when using the relay function, select Require TLS/SSL and authenticate only the relay .
Authentication	If you want to permit only the users on the authorized list to log on to SMTP, select Verify IDs on local delivery .
Authentication	If you want the SMTP server to allow the mail server framework (MSF) snap-in functions to reject an e-mail that is not verified, select Verify message originator .
Authentication	If you want the SMTP server to verify whether the e-mail address of the sender is in the system distribution directory and if the addresses match, select Users or Users not on the accept list . The users whose e-mail addresses cannot be matched are rejected.

4. Click **OK** to accept the changes.

Related tasks

“Restricting the relay of messages” on page 25

To prevent people from using your e-mail server for spamming or sending large amounts of bulk e-mail, you can use the relay restriction function to specify who can use your system for relaying messages. However, you cannot authenticate your e-mail when you restrict relaying messages.

“Configuring the Simple Mail Transfer Protocol server” on page 15

When you configured TCP/IP, the system automatically configured SMTP for you. However, you still need to change a few SMTP properties to ensure that the SMTP server works correctly for e-mail.

Tracking the e-mail sender

You can now set the SMTP server to reject an e-mail sender who is not authenticated. In addition, you can set the snap-in functions of the SMTP mail server framework (MSF) to reject an e-mail that is not verified.

You need to enable transaction encryption, that is, TLS/SSL protocols, to reject an unverified sender or e-mail.

| Rejecting an e-mail sender who is not verified

| To reject e-mail senders who are not verified, follow these steps:

- | 1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
- | 2. Right-click **SMTP** and select **Properties**.
- | 3. Click the **Authentication** tab.
- | 4. If you want to verify all the e-mail senders, in the **Verify mail from user** field, select **All**. Select **Users not on the accept list** if you only want to verify the users that are not on the accept list.
- | 5. Click **OK**.

| The SMTP server checks to see whether the sender is in the System Distribution Directory and if the e-mail address matches the one in the directory. If there is a mismatch, the user is rejected.

| Rejecting an e-mail that is not verified

| To reject an e-mail that is not verified, follow these steps:

- | 1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
- | 2. Right-click **SMTP** and select **Properties**.
- | 3. Click the **Authentication** tab.
- | 4. Select **Require TLS/SSL and authenticate it locally and when using the relay** for the **Allow authentication** field.
- | 5. Select **Verify MSF message originator**.
- | 6. Click **OK**.

| If the e-mail does not come from an authenticated source, then the user that issued the QzmfCrtMailMsg() API should be the originator of the MSF message. Otherwise, the SMTP snap-in functions reject the e-mails.

Restricting the relay of messages

| To prevent people from using your e-mail server for spamming or sending large amounts of bulk e-mail, you can use the relay restriction function to specify who can use your system for relaying messages. However, you cannot authenticate your e-mail when you restrict relaying messages.

You have six options for allowing relays:

- Allow all relay messages
- Block all relay messages
- Accept relay messages for only recipients in the near domains list
- Accept relay messages from only the address relay list
- Accept relay messages using both the near domains and address relay lists
- Accept relay messages from POP clients for a specified period of time

| You can now restrict relays only when you select the **No TLS/SSL and no authentication will be done** option. In System i Navigator, the option is on the Authentication page when you specify SMTP properties.

To specify users that can send e-mail to the Internet, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Click the **Relay Restrictions** tab.
4. Select the appropriate relay restriction from the options offered here.

Note: If you choose **Accept relay messages for only recipients in the near domains list** or **Accept relay messages using both the near domains and address relay lists**, then you need to click the **General** tab to list the near domains from which you are accepting relays.

5. Click **OK**.

Related concepts

“Controlling e-mail access” on page 10

You need to control who accesses your system through e-mail to protect your data from malicious attacks.

Related tasks

“Authenticating e-mail for local and relay” on page 24

You can now prevent your server from spam by requiring authentication to send e-mail. You cannot require authentication if you want to restrict relaying messages. It is recommended that you set up authentication for your server.

Related reference

Change SMTP Attributes (CHGSMTPA) command

Accepting relay messages from Post Office Protocol clients

One of the options for relay restriction enables Post Office Protocol (POP) clients to relay messages through Simple Mail Transfer Protocol (SMTP) for a specified period of time after they log on to the POP server.

This function is commonly called POP before SMTP. It is particularly useful for mobile employees that use dynamic IP addresses, because security checking functions that use fixed IP addresses are not effective for checking dynamic IP addresses. You can enable a mobile employee to authenticate once to the POP server and to send e-mail for a designated period of time (15 - 65535 minutes) without authenticating again.

For example, you might configure the system to allow your remote users to relay messages through the SMTP server during a four-hour (240 minutes) period of time after they log on to the POP server. In this example, a mobile worker logs on to the POP server to retrieve his e-mail. The POP server records the user's IP address and a time stamp in a queue. An hour later, the user decides to send an e-mail message. When the user sends the e-mail message using SMTP, the SMTP server checks the queue to verify that the user accessed the POP server to retrieve e-mail sometime during the configured time period. After the user is verified, the SMTP server relays the e-mail message to the SMTP client for delivery to the e-mail recipient.

Note: To more precisely control the users that can access your e-mail server, you can use the relay restriction function and the connection restriction function together. For example, you might want to restrict specific groups of users from connecting to your e-mail server but allow certain POP clients within that group to use your SMTP server to send e-mail messages.

To enable POP clients to relay messages for a specified length of time, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Click the **Relay Restrictions** tab.
4. For **Allow relay messages**, select **Specified**.
5. Select **From the POP client for the following duration (15 - 65535)** and enter a time value to specify the number of minutes to allow a client to send mail using the SMTP server.
6. Click **OK**.

Using relay restriction and connection restriction functions together

The i5/OS operating system enables you to use the relay restriction function along with the connection restriction function to carefully control who can access your e-mail server.

You can restrict specific groups of users from connecting to your e-mail server but allow certain Post Office Protocol (POP) clients within that group to use your SMTP server to send e-mail messages.

For example, you know that users within a specific range of IP addresses routinely send spam e-mail. Therefore, you want to restrict addresses in that range from connecting to your e-mail server. However, several of the IP addresses in the IP address range represent trusted i5/OS users, and you want to enable those users with i5/OS user profiles to relay messages for a specified period of time after they log on to the POP server.

Fortunately, you can use the connection restriction function to restrict connections of the specific range of IP addresses, and use the relay restriction function to allow certain trusted users (POP clients) within the restricted range to send e-mail using your Simple Mail Transfer Protocol (SMTP) server. The i5/OS operating system first checks to see if you configured the system to allow POP clients to relay messages for a specified period of time. Then, it checks for restricted connections. This i5/OS capability enables you to precisely control who can use your SMTP server to relay messages and who can connect to your e-mail server.

- | If you choose to use the connection restriction function and the relay restriction function together, you
- | need to specify OVERRJTNNL(*YES) (Override reject connect list) on the Change SMTP Attributes
- | (CHGSMTPA) CL command. This parameter enables the POP server authentication capability to override
- | the connection restriction configuration. At a later date, you might want to remove the relay restriction
- | that allows the POP clients within the restricted group to use your e-mail server. In that case, you need to
- | specify OVERRJTNNL(*NO) on the CHGSMTPA command.

Related tasks

“Restricting connections”

To ensure the security of your system, you need to prevent the connection of users who might abuse your e-mail server.

Related reference

- | Change SMTP Attributes (CHGSMTPA) command

Restricting connections

To ensure the security of your system, you need to prevent the connection of users who might abuse your e-mail server.

Unwanted users might connect to your system and send unsolicited mail. This unsolicited e-mail takes a great amount of processing unit cycles and space. Also, if your system allows others to relay unsolicited mail, other systems might block the mail that comes from your system.

You can specify IP addresses of known unwanted users, or you can connect to a host that contains a Realtime Blackhole List (RBL) server. These Realtime Blackhole Lists provide a listing of known IP addresses that send unsolicited mail.

To specify known IP addresses or a host with a Realtime Blackhole List, complete the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Click the Connection Restrictions page.
4. Click **Add** to add host names of servers with Realtime Blackhole Lists that you would like to use.
5. Click **Add** to add specific IP addresses to restrict attempted connections.
6. Click **OK**.

Related concepts

“Controlling e-mail access” on page 10

You need to control who accesses your system through e-mail to protect your data from malicious attacks.

Related tasks

“Using relay restriction and connection restriction functions together” on page 26

The i5/OS operating system enables you to use the relay restriction function along with the connection restriction function to carefully control who can access your e-mail server.

Filtering e-mail to prevent virus proliferation

To prevent the spread of a virus that might infiltrate the e-mail servers, you can create filters to look for a particular subject, type, file name, and originator’s address in incoming e-mail. The e-mail can then be quarantined or discarded.

With virus filtering, questionable e-mails are automatically quarantined or discarded based on parameters established by the administrator. E-mails can be filtered by any or all of the following criteria:

1. **Address**-individuals or domains
2. **Subject** - ILOVEYOU
3. **Attachment name** - lovebug.vbs or *.vbs
4. **MIME type** - image/* or image/jpg

The values can contain wildcard characters. One wildcard character is an asterisk (*), which specifies that one or more arbitrary characters can be at the position of the wildcard. For example, *.vbs can be used to check for filenames with an extension of .vbs. An originator of *@us.ibm.com filters all mail from IBM in the United States, and a filter of image/* filters type image for all subtypes.

To create a filter, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Select the **Filters** page.
4. Select **Keep message** or **Discard message**. Selecting **Keep message** will save a copy of the message, which will not be delivered to the recipient.
5. Click **Add** to specify the message criteria that identifies the potential virus. Messages matching this criteria will not be delivered to the recipient.
6. Click **OK** to save your changes.

In addition to these tools, you need to implement supplemental antivirus solutions.

Sending and receiving e-mail

Your system is a mail server and has e-mail users (SNADS, POP, or Lotus users) enrolled on it. Your e-mail users can send, receive, and read e-mail using either a POP client or a SNADS client.

| Your users can use the Send MIME Mail (QtmmSendMail) API or the Create and Send MIME Email (QtmsCreateSendEmail) API to send e-mail from an i5/OS program. By using the QtmsCreateSendEmail API, the users can sign and encrypt the MIME document using secure/MIME, which is a secure version of the MIME protocol. The QtmsCreateSendEmail API is the preferred way to send e-mail programmatically.

| In addition, your users can send and receive e-mail in the following different ways.

Related concepts

“E-mail concepts” on page 2

You depend on electronic mail (e-mail) as an essential business tool. The i5/OS operating system uses

protocols, like Simple Message Transfer Protocol (SMTP) and Post Office Protocol (POP), to make your e-mail run smoothly and efficiently on the network.

Related tasks

“Enrolling e-mail users” on page 18

You need to create user profiles to enroll e-mail users.

Related reference

Create and Send MIME E-mail (QtmsCreateSendEmail) API

Send MIME Mail (QtmmSendMail) API

Setting up Post Office Protocol e-mail clients

If you want to receive and store e-mails by using the Post Office Protocol (POP) server, you need to set up an e-mail client first.

- | Your system uses the POP server to store and forward e-mail. The e-mail client works with the POP
| server to receive and store e-mails for the users on the client side. A number of e-mail clients are
| available to support POP including Eudora, Outlook Express, and Lotus Notes®. The steps you must take
| to configure the client are specific to that client’s interface. However, the information that you must
| provide is the same. These steps, using Outlook Express as an example, are as follows:
1. Gather POP e-mail client program information.
 - User ID and a fully qualified domain name (the host name plus the domain name). This is the user’s e-mail address for receiving mail and is typically in the form of `userID@hostname.domainname`.

Note: On some clients, you might have to enter the host address several times: to specify the POP server’s host for receiving mail, to specify SMTP’s host for sending mail, and to identify the sender of the e-mail to the recipients.

 - POP user or account name. This is the same as the i5/OS user profile name.
 - The user password. This password must be the same as the i5/OS user profile password.
 - | 2. Identify the user and the user’s preferences. In Outlook Express, for example, click **Tools** → **Accounts**,
| and then click the **Mail** tab to identify the information about the user and the user’s preferences.
 - User name. This is the i5/OS user profile name.
 - User’s e-mail address. This is the user ID and fully qualified domain name.
 - Reply-to address. This can be the same as the user’s e-mail address that the network administrator designates, but an i5/OS user profile must exist on the system.
 - | 3. Identify the outgoing mail (SMTP) server. You need to identify the SMTP server on the e-mail client
| because it is the server that allows the client’s users to send mail out. In Outlook Express, for
| example, click **Tools** → **Accounts**, select the e-mail account and click **Properties**. Click the **Servers** tab
| and identify the SMTP server.
 - POP user or account name. This is the user ID on the user’s e-mail address; it is also the i5/OS user profile name.
 - Outgoing mail (SMTP) server. This is the system host name.
 - | 4. Identify the incoming mail (POP) server. In Outlook Express, for example, click **Tools** → **Accounts**,
| select the e-mail account, and click **Properties**. Click the **Servers** tab and identify the POP server.
 - Incoming mail server. This is the system host name.
 - | 5. Configure the client program to use TLS/SSL. In Outlook Express, for example, follow these steps for
| configuration:
 - a. Click **Tools** → **Accounts** and select the e-mail account.
 - b. Click **Properties** and then click the **Servers** tab.
 - c. Select **My server requires authentication** and click **Settings**.
 - d. Select **User name settings as my incoming mail server** and click **OK**.

- | e. Click the **Advanced** tab and select **This server requires a secure connection (SSL)** for both the Incoming (POP) and Outgoing (SMTP) mail servers. Click **OK**.
- | f. Click **Apply** and then **OK** to close the Properties window.

JavaMail

You can develop e-mail client applications by using JavaMail.

The JavaMail API provides a platform-independent and protocol-independent framework you can use to build Java™ technology based e-mail client applications. You can use the JavaMail API to create a mail client capable of sending multimedia mail messages, as well as enabling the implementation of Internet Mail Access Protocol (IMAP), which supports folders, authentication, and attachment handling.

Because SMTP only supports character data, it uses MIME to represent complex data, such as formatted text, file attachments (text and binary), and multimedia content. If you use the Send MIME Mail (QtmmSendMail) API, your application must take care of converting the data into the appropriate content. The JavaMail implementation provides integrated MIME processing capabilities.

JavaMail components are included as part of the IBM Developer Kit for Java.

Related concepts

JavaMail

Sending spooled files as PDF files

You can send spooled files in Adobe Portable Document Format (PDF) and distribute the documents by e-mail.

Using the IBM Infoprint® Server for iSeries™ licensed program (5722-IP1), you can produce Adobe PDF files from any i5/OS output. You can send these generated PDF files as e-mail attachments. You can send a single spooled file to an address. You can also split up a spooled file into several PDFs and send each one to a different address. Using this method, you can send customer invoices to separate PDF files and send the appropriate invoice to each customer's e-mail address. The IBM Infoprint Server for iSeries licensed program is required to use this output method.

Related information



InfoPrint Server User's Guide PDF



IBM eServer iSeries Printing Redbooks VI -- The Output of e-business

Using Lightweight Directory Access Protocol for addresses

You can use Lightweight Directory Access Protocol (LDAP) to provide a public address book based on the system distribution directory.

- | You can use IBM Tivoli® Directory Server for i5/OS (which is the IBM implementation of LDAP) to replace the function previously served by MAPI. Using LDAP, you can provide a single address book that
- | can be accessed by all users from the client application.

To use LDAP, complete the following tasks:

1. Start the Directory Server.
2. Publish information to the Directory Server.
3. Configure your mail client to use LDAP. The steps to complete this task will depend on your mail client (Netscape or Eudora, for example). Edit the properties in your mail client to specify the LDAP server as the Directory Server for mail addressing.

Related tasks

Getting started with Directory Server
Publishing information to the directory server
Related reference
IBM Tivoli Directory Server for i5/OS (LDAP)

Sending e-mail using Systems Network Architecture distribution services

You can send e-mail from your system using a Systems Network Architecture distribution services (SNADS) client program. The sender of the e-mail must be a local SNADS user.

Prerequisites

A local SNADS user must have a user profile so that the user is enrolled in the local system distribution directory entry. To enroll local SNADS e-mail users, see *Enrolling e-mail users*.

To send e-mail, follow these steps:

1. In the i5/OS character-based interface, type SNDDST (the Send Distribution command) and press Enter.
2. Press F10 to see all the parameters.
3. At the first prompt, *Information to be Sent*, enter *LMSG and press Enter.
4. Enter the recipient's user ID and server address or an Internet address.
5. Enter a message description at the *Description* prompt.
6. Press the Page Down key and type your e-mail at the *Long Message* prompt.
7. Press Enter to send the e-mail.

Note: You can also use Internet addressing when you send mail with the Send Distribution (SNDDST) command.

Related tasks

"Enrolling e-mail users" on page 18

You need to create user profiles to enroll e-mail users.

"Receiving e-mail using Systems Network Architecture distribution services" on page 33

You can receive e-mail on your system using a Systems Network Architecture distribution services (SNADS) client program. The recipient of the e-mail must be a local SNADS user.

Setting up headers to differentiate between recipients

The Change Distribution Attributes (CHGDSTA) command changes the content of message services attributes (X.400 support) for mail distributions.

The Keep Recipient (KEEPRCP) parameter specifies which recipient information is stored and sent within each mail distribution. The setting of this parameter affects how the MIME headers get created for a note from SNDDST.

In order for CC and BCC tags to show up in MIME headers (and client screens), you must set the KEEPRCP parameter to *ALL. BCC recipients are not shown regardless of the setting of this parameter because they are not intended to be. The TO and CC recipients show up in the text of the SNDDST note.

Multipurpose Internet Mail Extension content types

Standard Internet text notes consist of a general header and a text body. Multipurpose Internet Mail Extension (MIME) notes, however, can contain multiple parts, which allow multimedia attachments to be included with the text.

```

From
@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com Wed
Jan 10
11:33:18 1996 Return-Path:
<@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com> Received: from
SYSNAM6.city.company.com by
fakeps2.city.company.com (COMPANY
OS/2 SENDMAIL VERSION 1.3.2)/1.0) id AA0329; Wed, 10
Jan 96 11:33:18 -0500 Date: Wed, 10
Jan 96
11:33:18 -0500 Message-Id: <9601101633.AA0329@fakeps2.city.company.com> Received:
from endmail9 by SYSNAM6.CITY.COMPANY. (IBM i5/OS SMTP V03R02M00) with TCP;
Wed, 10
Jan 1996 10:23:42
+0000. X-Sender: popct08@SYSNAM6.city.ibm.com (Unverified) X-Mailer: Windows
Eudora Pro
Version 2.1.2
Mime-Version: 1.0Content-Type:multipart/mixed;boundary="===== _821301929==
"
To: fake@fakeps2.city.company.com From:
endmail9 <popct08@SYSNAM6.city.company.com> Subject:
eudora attachments
X-Attachments:C:\EUDORA\ARGYLE.BMP;----- _821301929==
Content-Type: text/plain; charset=

"us-ascii" An example of using Eudora to send a text
andbitmap.----- _821301929==
Content-Type: application/octet-stream; name="ARGYLE.BMP";
x-mac-type="424D5070"; x-mac-creator="4A565752"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=

```

Figure 2. Example of a multipart MIME note

You can send e-mail to the Internet with the SNDDST command by entering an Internet e-mail address at the *Internet Recipient* prompt.

Follow these steps to configure your mail system:

- Now your SNADS users can send e-mail to the Internet with the SNDDST command by entering an Internet e-mail address at the *Internet Recipient* prompt.

32 System i: Networking E-mail

Attaching files

When sending e-mail using the SNDDST command, you might want to send a file or document with the e-mail.

You can send e-mail with an attached file or document by using the Send Distribution (SNDDST) command. SNDDST is only capable of sending a single document or file at a time. If you would like to send multiple attachments, send MIME mail with the Send MIME Mail (QtmmSendMail) API.

To attach and send a *document* with your e-mail, in the character-based interface, type:

```
SNDDST TYPE(*DOC) DSTD(your description) TOUSRID(anyuser) DOC(yourdoc) FLR(yourfolder)
```

To attach and send a *file* with your e-mail, in the character-based interface, type:

```
SNDDST TYPE(*FILE) DSTD(description) TOUSRID(any user)  
MSG(message optional) DOCFILE(youlib/yourfile) DOCMBR(yourmbr)
```

If you receive error messages, you might be attempting to send a file or document that is in a format that is not compatible with the Send Distribution (SNDDST) command. You can use the i5/OS CL CPY commands to convert the file to a file or document that is compatible with the SNDDST command.

Converting file types to send with SNDDST

Assuming that the spooled file is already created, and the physical file and folder already exist, you must convert the file into a required format for sending.

1. Move the spooled file to a database physical file:

```
CPYSPLF FILE(splfile) TOFILE(dbfile) JOB(job3/job2/job1) SPLNBR(splnbr) TOMBR(mbr)
```

2. Move the physical database file to a folder:

```
CPYTOPCD FROMFILE(lib/dbfile) TOFLR(folder) FROMMBR(mbr) REPLACE(*YES)
```

3. Send the document:

```
SNDDST TYPE(*DOC) TOUSRID(user address) DSTD(MAIL) DOC(mbr) FLR(folder)
```

Related reference

Send MIME Mail (QtmmSendMail) API

Receiving e-mail using Systems Network Architecture distribution services

You can receive e-mail on your system using a Systems Network Architecture distribution services (SNADS) client program. The recipient of the e-mail must be a local SNADS user.

To receive e-mail, follow this procedure.

1. In the character-based interface, type QRYDST (the Query Distribution command) and press F4. The list of distributions appears.
2. Press F10 to view additional parameters.
3. In the **File to Receive Output** field, type file and library names that are easy to remember and press Enter. The system creates these physical files.
4. Type WRKF (the Work with Files command) and press Enter. The Work with Files display appears.
5. Type the file name and library you specified in step 3 and press F4.
6. The display lists all your distributions (e-mail). Type 5 next to the distribution you want to display and press Enter.
7. At the Display Physical File Member (DSPPFM) display screen, press Enter.

8. On the next display screen, there will be a long string of numbers for each piece of mail. Copy the seventh through twenty-sixth characters.
9. Press F3 twice to exit.
10. Type RCVDST (the Receive Distribution command) and press Enter.
11. In the **Distribution Identifier** field, paste the seventh through twenty-sixth characters you copied.
12. In the **File to receive output** field, enter a new file name and the same library name you used previously and press Enter.
13. Type DSPPFM (Display Physical File Member) to display the file you just created.
14. Press F20 (Shift + F8) to scroll left and read the message or messages.

Related tasks

“Sending e-mail using Systems Network Architecture distribution services” on page 31

You can send e-mail from your system using a Systems Network Architecture distribution services (SNADS) client program. The sender of the e-mail must be a local SNADS user.

Managing e-mail

As an experienced user or administrator, you can manage e-mail servers, users, and messages to ensure distribution of e-mail in your network.

Checking e-mail servers

One of the most common problems with e-mail is that the proper servers are not started. Before using your e-mail servers, you need to verify the status of e-mail servers and make sure that they are all running.

To verify the status of the servers, complete these steps:

1. In System i Navigator, expand *your system* → **Work Management** → **Server Jobs**.
2. Verify that the SMTP server is active. Find **Qtsmtp** jobs in the Job Name column of the Active Server Jobs list.
3. If there are no **Qtsmtp** jobs listed, start the SMTP servers.
4. Verify that the Mail Server Framework server is active. Find **Qmsf** jobs in the Job Name column of the Active Server Jobs list.
5. If there are no Qmsf jobs listed, type STRMSF (the Start the Mail Server Framework command) in the character-based interface.
6. Verify that the POP server is active. Find **Qtpop** jobs in the Job Name column of the Active Server Jobs list.
7. If there are no **Qtpop** jobs listed, start the POP servers.
8. Verify that the SNADS server is active. Find **Qsnads** jobs in the Job Name column of the Active Server Jobs list.
9. If no QSNADS jobs are listed, start SNADS. In the character-based interface, type STRSBS QSNADS.

All your e-mail servers must be started for e-mail to work.

Related concepts

“Starting and stopping e-mail servers” on page 19

Start the required servers to ensure that everything works properly and that all the configuration changes you made take place. Sometimes, it might be necessary for you to restart the servers. This can be done by stopping the servers, and then completing the steps to start the servers again.

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Removing Post Office Protocol e-mail users

You can remove Post Office Protocol (POP) e-mail users by using System i Navigator.

To remove an e-mail user from the operating system, you must delete this system distribution directory entry as follows:

1. In the character-based interface, type WRKDIRE (the Work with Directory Entries command).
2. Tab down until you are in the *Opt* field by the user you want to delete.
3. Type a 4 (Remove) and press Enter. Press Enter again to confirm. This prevents any more e-mail from being delivered to the user's POP mailbox.
4. Sign on to a POP mail client program as that user. Receive and delete any e-mail.

Preventing large e-mail messages from splitting

You might need to prevent your large e-mail messages from splitting, and being delivered in smaller, confusing pieces.

Simple Mail Transfer Protocol (SMTP) can be configured to split large messages into smaller pieces. However, many mail clients cannot reassemble the pieces, resulting in unreadable messages. If you find that your recipients cannot read large messages because they are broken into several pieces, you might want to disable the SMTP splitting function.

To disable SMTP e-mail splitting, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **POP**. The POP Properties dialog appears.
3. Click the **Configuration** tab.
4. For the **Message Split Size** field, select **No maximum**.

Note: Turning e-mail message splitting off might cause problems when sending large e-mail to networks that cannot handle large messages.

Related concepts

“Troubleshooting e-mail” on page 45

This information is designed to help you solve problems related to e-mail that you might experience.

Receiving delivery status of e-mail

If your users would like to receive messages on the delivery status of their outgoing e-mail, you must enable the delivery status notification function.

Delivery status notification allows your e-mail clients to receive status messages when e-mail is delivered, relayed, or fails. If you want to allow your e-mail clients to make this request, you must enable delivery status notification.

You are only enabling the delivery status notification function for your users. If users want to use the delivery status notification function, they must set the parameters in their mail clients. The parameters vary from mail client to mail client.

To enable delivery status notification, complete the following steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Click the Additional Parameters page.
4. Select the **Support Delivery Status Notification (DSN)** check box, and specify DSN notification Responsible Person address.
5. Click **OK**.

Using the delivery status notification function takes up resources that can affect the maximum number of recipients on a piece of e-mail.

Hosting a Domino and SMTP server on the same system

If you are running Domino and Simple Mail Transfer Protocol (SMTP) on the same system, it is suggested that you configure each one to bind to a specific IP address.

When hosting Domino and SMTP servers on the same system, you should bind each server to an IP address. E-mail is then sent to users of Domino or SMTP using the appropriate IP address and although it shares a port, the e-mail is only handled by the system for which it is intended.

To force the SMTP server to use a specific Internet address, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **SMTP** and select **Properties**.
3. Click the **Bindings** tab.
4. Select the **Use all interfaces** radio button to bind all interfaces to port 25.
5. Select the **Select an interface** radio button to specify the client and server bound interfaces that you would like to bind.

Note: If you want to use network address translation (NAT) either on the system or on your firewall, you must force the i5/OS SMTP client to use one specific Internet address.

6. Click **OK**.

Now, SMTP receives only mail that is addressed to this Internet address. Check the Domain Name System (DNS) server, local host table, and system distribution directory to ensure that this forced Internet address is present.

Refer to the Lotus Domino Reference Library  for instructions on how to bind Domino SMTP to a specific TCP/IP address.

Related concepts

“Planning for e-mail” on page 9

Before setting up e-mail, you must have a basic plan for how to use e-mail on your system.

IP filtering and network address translation (NAT)

Hosting Domino LDAP and Directory Server on the same system

If you are running Domino LDAP and IBM Tivoli Directory Server for i5/OS (Directory Server) on the same system, it is suggested that you configure each one to bind to a specific IP address.

When hosting Domino LDAP and Directory Server on the same system, you can either set a different port number for each server or you can bind each server to an IP address. Changing the port number can be disruptive to your clients, so specifying a specific IP address for each server might be the best solution. Domino and Simple Mail Transfer Protocol (SMTP) each use the appropriate LDAP server for e-mail addressing.

To force the Directory Server to use a specific Internet address, follow these steps:

1. In System i Navigator, select *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **Directory** and select **Properties**.
3. Click the **Network** tab.
4. Click **IP Addresses**.
5. Select **Use selected IP addresses** and specify from the list which interfaces you want to bind.
6. Click **OK** to close the Directory - IP Addresses page.

7. Click **OK** to close the Directory Properties page.
8. Optional: If you are using Domino LDAP, see the Lotus Domino Reference Library for instructions on how to bind Domino LDAP to a specific TCP/IP address.
9. Start the servers for e-mail.

Related information

 Lotus Domino Reference Library

Managing Simple Mail Transfer Protocol server performance

These are tips for managing a busy Simple Mail Transfer Protocol (SMTP) server that uses multiprocessing.

Your SMTP server might be busy because it uses all its capacity for adding and ending prestart jobs for each e-mail request.

If you find that the number of prestart jobs affects system performance, you can set the threshold lower. If you want more jobs, you can set the number of prestart jobs higher.

With prestart jobs, every e-mail request runs as its own job. This method allows each job to focus solely on its client or server program's needs and requests. Each job can make longer time-out calls to enable the posting of host names for the purpose of not receiving unsolicited bulk e-mail.

To manage a busy SMTP server, you can change the following values:

- The number of jobs to start on initialization
- A threshold number for jobs
- The number of jobs to add when the system reaches the threshold
- A maximum for the number of running jobs to allow
- Selecting a subsystem for jobs

To manage a busy system, you need to change values on the SMTP server and the SMTP client.

The SMTP server works with the daemon and prestart jobs: QTSMTPSRVD and QTMSMTPSRVP. The SMTP client works with the daemon and prestart jobs: QTSMTPCCLTD and QTSMTPCCLTP.

To change the values on the SMTP server, follow these steps:

1. In the character-based interface, type CHGPJE (the Change Job Entries command).
2. Enter the following values at the prompt and press Enter.

Prompt	Value
Subsystem	QSYSWRK
Library	QSYS
Program	QTMSSRCP
Library	QTCP
Start jobs	*SAME
Initial number of jobs	4
Threshold	2
Additional number of jobs	2
Maximum number of jobs	20

These values guarantee that the system starts four prestart jobs, starts two additional jobs when the available jobs fall below two, and allows a maximum of 20 prestart jobs.

Changing values for the Simple Mail Transfer Protocol server

Use this procedure to change the values on the Simple Mail Transfer Protocol (SMTP) server.

1. In the character-based interface, type CHGPJE (the Change Job Entries command).
2. Enter the following values at the prompt and press Enter.

Prompt	Value
Subsystem	QSYSWRK
Library	QSYS
Program	QTMSSRCP
Library	QTCP
Start jobs	*SAME
Initial number of jobs	4
Threshold	2
Additional number of jobs	2
Maximum number of jobs	20

These values guarantee that the system starts four prestart jobs, starts two additional jobs when the available jobs fall below two, and allows a maximum of 20 prestart jobs.

Changing values for the Simple Mail Transfer Protocol client

Use this procedure to change the values on the Simple Mail Transfer Protocol (SMTP) client.

1. In the character-based interface, type CHGPJE (the Change Job Entries command).
2. Enter the following values after the prompt and press Enter.

Prompt	Value
Subsystem	QSYSWRK
Library	QSYS
Program	QTMSCCLCP
Library	QTCP
Start jobs	*SAME
Initial number of jobs	4
Threshold	2
Additional number of jobs	2
Maximum number of jobs	20

These values guarantee that the SMTP client starts four prestart jobs, starts two additional jobs when the available jobs fall below two, and allows 20 prestart jobs as the maximum.

Selecting a new subsystem for Simple Mail Transfer Protocol server jobs

Use this procedure to select a new subsystem for Simple Mail Transfer Protocol (SMTP) server jobs.

1. You can specify a separate subsystem for the SMTP server. This should increase performance, because the need to share resources is eliminated.
2. To specify a separate subsystem, complete the following steps:
 - a. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. Right-click **SMTP** and select **Properties**.

- c. Click the **Additional Parameters** tab.
- d. Select the **Subsystem description** radio button.
- e. Enter the new subsystem's name and the library where the subsystem description and job queue will be created.

The program will check for existence of the specified subsystem. If it does not exist, the program will create it along with routing table entries, auto-start job entries, pre-start job entries and job descriptions. Even if the subsystem does not already exist, the library for the subsystem description and job queue must already exist. When the startup job for the server is processed, it will specify the parameters for the newly created subsystem and then submit the server jobs for batch startup in that subsystem.

E-mail reference information

You can find reference information about mail server journal entries, Simple Mail Transfer Protocol (SMTP) commands, and Post Office Protocol (POP) verbs and parameters.

Mail server journal entries

Use this information to help you understand the codes and messages used in journal entries.

The following tables provide more detailed information about reading the journal entries.

- "Journal entry abbreviations"
- "Log entries for the SMTP client" on page 40
- "Log entries for the SMTP server" on page 41
- "Log entries for the bridge server" on page 41
- "Message Switching Facility (MSF) exits and creates functions" on page 42

Journal entry abbreviations

Abbreviation	Definition
LIN	Local in, received a note for local delivery. The IP address that follows is the host that sent the note.
RIN	Relay in, received a note to relay to another SMTP daemon. The IP address that sent it follows.
R	Recipient
O	Originator
U	Undelivered recipient
QTMSINQ	Input queue of SMTP
QTMSOUTQ	Output queue of SMTP
QTMSBSSQ	Holding queue where messages are placed when system storage threshold is exceeded.
QTMSRTQ1	First level retry queue
QTMSRTQ2	Second level retry queue
RRSL	Recipient resolved

Each journal entry has a 2-character subtype or code preceding it. The first character of the subtype or code consists of the function identifier for the entry. The second character of the subtype or code consists of the action that this journal entry is documenting. The function identifiers are listed in the following table.

Function identifier	Description
7	Bridge Server Entry
8	SMTP Client
9	SMTP Server
A	MSF Non Delivery
B	MSF Local Delivery
C	MSF Message Forwarding
D	POP Create Message
E	Send Mail API
F	Domino MTA
G	Tunneling Snap-in
H	SNADS (Switcher)
I	MIME Parser (a local delivery snap-in)
L	FAX (Local Delivery)
M	SNADS
O	Filtering
P	MSF SMTP exit for Address Resolution

All of the journal entries documented here use the log entry (LG) type.

Log entries for the SMTP client

Type	Action	Subtypes or codes	Comments
LG	Dequeuing of container for processing	8B	Just after floater tag is set log dequeue of Mail.
LG	Successful mail delivery	88 82	Log mail successfully sent. Log each recipient.
LG	Undeliverable mail	83	Log undelivered mail.
LG	1st level timeout	8C	Log when adding to 1st level retry queue.
LG	2nd level timeout	8D	Log when adding to 2nd level retry queue.
LG	Mail is ready to be retried	8E 8F	Log when retried mail put back on QTMSOUTQ.
LG	COD being sent back to originator	87	Log when confirm on delivery (COD) is enqueued on BRSR queue.
LG	Cannot process, resource busy	86	Log when mail gets put back on QTMSOUTQ because connection matrix is full.
LG	Examine recipient records	86	Log when mail gets put back on QTMSOUTQ because the recipient status changed, that is, the MS record resolved ready to deliver the message.

Type	Action	Subtypes or codes	Comments
LG	Undeliverable	87	Log transfer of mail to QTMSINQ for undelivered notice in two places.
LG	MX query	8K	Log a res_send failure and errno of why if failed along with query buffer.

Log entries for the SMTP server

Type	Action	Subtypes or codes	Comments
LG	Receiving mail	94 91 92 9T 99	Log reception of mail just after receiving ending sequence CRLF <.> CRLF (local). Originator and recipient are logged. Message size <i>nnnnn</i> where <i>nnnnn</i> is the number of bytes. MSGID
LG	Receiving relayed mail	95 91 92	Log MAIL just after receiving ending sequence CRLF <.> CRLF (relayed). Originator and recipient are logged.
LG	Passing off mail to Bridge server	97	Log entry of MAIL into QTMSINQ (incoming mail).
LG	Passing off mail to client for remote delivery	96	Log entry of MAIL into QTMSOUTQ (relayed mail).
LG	CONNECTION REFUSED 1.2.3.4....	9S	Log connections refused based on restricted connection settings. 1.2.3.4 is the IP address rejected.
LG	RELAY REFUSED 1.2.3.4....	9V	Log relays refused based on restricted relay settings. 1.2.3.4 is the IP address rejected.
LG	Rejected by SMTP server	9W	The message has been rejected by the SMTP server.

Log entries for the bridge server

Type	Action	Subtypes or codes	Comments
LG	Getting mail off of the IN queue	7A	Log mail being dequeued from QTMSINQ.
LG	Passing off mail to SNADS	7O	Record successful transfer to QSNADS.
LG	Putting container on the BUSY queue because of space usage	7L	Record when mail is enqueued on QTMSBSSQ because of threshold overflow.

Type	Action	Subtypes or codes	Comments
LG	Getting mail off of BUSY queue	7M	Record dequeuing mail from QTMSBSSQ. Space was reclaimed and the mail can now be processed.
LG	Passing message to MSF	7H 71 72	Record when message gets inserted into framework.
LG	Creation of COD message	7R 7G	Record when COD message gets inserted into framework. Log the MSF MSGID because the new COD message is being created.
LG	Cannot deliver this piece of mail to a recipient	7P 7G	Log the fact that you were creating an undeliverable notice. Log the MSGID of the new undeliverable message notice.

Message Switching Facility (MSF) exits and creates functions

Type	Action	Subtypes or codes	Comments
LG	Creation of nondelivery message	AP A1 A2	Record nondelivery message being inserted into MSF.
LG	Mail is delivered into a POP mail box	B8 B2	Record delivery of message to local pop mail box. The ipaddress is the pop mailbox directory. Recipient is also listed.
LG	Sending COD message into MSF	BR B1 B2	Record insertion of COD message into the MSF.
LG	Checking availability	CN	SMTP message Forwarding MSF exit. Record MSGID that was put back on QMSF queue due to SMTP not being started.
LG	Enqueuing the mail	C6 C1 C2	Log mail being put onto QTMSOUTQ.
LG	Use of the Sendmail API	EH E1 E2 ET	Record creation of message by SendMail API. Message size <i>nnnnn</i> where <i>nnnnn</i> is size of message (all attachments).
LG	Mail is targeted to a SNADS bridged remote system	G8 G2	Record when message is tunneled. Include system sent to recipient.
LG	Mail tunneled through a SNADS bridge is received.	GQ G2	Record receiving tunneled message for local delivery recipient.

Type	Action	Subtypes or codes	Comments
LG	Address resolution SNADS switches either from/to	H1	SNADS switched a message into the MSF.
LG	Reinsertion of parsed MIME note into framework	IH I1 I2 IG	Log when the parsed MIME message is reinserted into the MSF.
LG	Rejected by Filtering	OW	Message has been rejected. Whether it was discarded or kept is noted. If it has been rewritten and delivered, that is noted.
LG	Typed by SMTP Address Resolution MSF exit program	P2	<p>Message has been tagged as follows:</p> <ul style="list-style-type: none"> • POP LclDel: Tagged for the POP local delivery exit program to deliver. • SMTP MsgFwd: Tagged for forwarding to SMTP to send. • SMTP NonDel: Marked for nondelivery notification. • Parse: Sent to the parser code. • PutBk: Put back into the framework for some other exit to handle (for example, Domino or SNADS). • chg to SNADS: Changed the address type to SNADS.

Related tasks

“Checking component journals” on page 47

You can check journals that record errors to determine how to solve a particular e-mail problem.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending and receiving e-mail. It is typically used with POP3 or Internet Message Access Protocol to save messages in a server mailbox and download them periodically from the server for the user.

SMTP commands

The following table describes the SMTP commands, the command functions, and whether the i5/OS SMTP server supports the commands.

SMTP command	What it does	System i supported
AUTH (Authentication)	Indicate an authentication mechanism to the SMTP server. Both PLAIN and LOGIN are supported.	Yes

SMTP command	What it does	System i supported
DATA (Data)	Consider the lines following the command to be e-mail from the sender.	Yes
EHLO (Extension Hello)	Enable SMTP extensions.	Yes
EXPN (Expand)	Ask the receiver to confirm that a mailing list has been identified.	No
HELO (Hello)	Identify the SMTP sender to the SMTP receiver.	Yes
HELP (Help)	Ask the receiver to send helpful information to the sender.	Yes
MAIL (Mail)	Start an e-mail transaction to deliver the e-mail to one or more recipients.	Yes
NOOP (Noop)	Ask the receiver to send a valid reply (but specify no other action).	Yes
QUIT (Quit)	Ask the receiver to send a valid reply, and then close the transmission channel.	Yes
RCPT (Recipient)	Identify an individual recipient of e-mail.	Yes
RSET (Reset)	End the current e-mail transaction.	Yes
SAML (Send and mail)	Deliver e-mail to one or more workstations and recipients if the user is not active.	No
SEND (Send)	Deliver e-mail to one or more workstations.	No
SOML (Send or mail)	Deliver e-mail to one or more workstations or recipients if the user is not active.	No
STARTTLS (Start Transport Layer Security)	Ask the SMTP server to start Secure Sockets Layer (SSL) or TLS negotiation with the SMTP client to establish an SSL or a TLS session.	Yes
TURN (Turn)	Ask the receiver to send a valid reply and then become the SMTP sender, or else ask the receiver to send a refusal reply and remain the SMTP receiver.	No
VERFY (Verify)	Ask the receiver to confirm that a user has been identified.	Yes

Related concepts

“Scenario: Sending and receiving e-mail locally” on page 4

This scenario demonstrates how e-mail is processed between local users.

Post Office Protocol

The Post Office Protocol (POP) Version 3 mail interface is defined in Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), and RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC is the mechanism used to define evolving Internet standards.

The client software uses commands called *verbs* to communicate with the POP server. The i5/OS POP server supports the following verbs.

Verb and parameters	Description
USER <id>	Pass user ID
PASS <password>	Password
STAT	Query mailbox
LIST <opt msg #>	Query message statistics
RETR <msg #>	Retrieve message
DELE <msg #>	Delete message
RSET	Reset message delete status
TOP <msg #> <lines>	Retrieve message header and data
UIDL <opt msg #>	Get message unique ID listing
NOOP	No operation
QUIT	Quit client session
CAPA	List capabilities
STLS	Start Transport Layer Security

Related concepts

“Scenario: Sending and receiving e-mail locally” on page 4

This scenario demonstrates how e-mail is processed between local users.

“Post Office Protocol on i5/OS” on page 4

The Post Office Protocol (POP) server is the i5/OS implementation of the Post Office Protocol Version 3 mail interface.

Troubleshooting e-mail

This information is designed to help you solve problems related to e-mail that you might experience.

Related tasks

“Preventing large e-mail messages from splitting” on page 35

You might need to prevent your large e-mail messages from splitting, and being delivered in smaller, confusing pieces.

Determining problems with e-mail

You can use simple steps to determine what is causing a problem with e-mail.

To identify likely sources of Simple Mail Transfer Protocol (SMTP) problems, follow these steps:

1. Verify that TCP/IP is configured for e-mail.
 - a. Ensure that any required PTFs are installed.
 - b. Check e-mail servers to ensure that the necessary servers are started and running.
2. Verify the local domain name.
 - a. In System i Navigator, expand *your system* → **Network**.
 - b. Right-click **TCP/IP Configuration** and select **Properties**.
 - c. Click the **Host Domain Information** tab and verify the local domain name.
3. Set the SMTP retry values lower.
 - a. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. Double-click **SMTP**.

- c. Click the **Outbound Mail Retries** tab.
4. Verify that the user ID and address of the receiver are in the system distribution directory.
 - a. In System i Navigator, expand *your system* → **Users and Groups** → **All Users**.
 - b. Right-click the **Profile** of the user ID and select **Properties**.
 - c. Click **Personal**, and go to the **Mail** tab to verify the address.
5. Verify whether a host table entry is necessary for the e-mail to reach the destination address.
 - a. In the character-based interface, type CHGTCPHTE (the Change TCP/IP Host Table Entry command) and enter the e-mail server's Internet address.
 - b. If no host table entry appears, then enter the host name for that Internet address.
6. Ensure you have not exceeded your storage threshold.
 - a. In System i Navigator, expand *your system* → **Configuration and Service** → **Hardware** → **Disk Units** → **Disk Pools**.
 - b. Right-click the source disk pool that you want to view and select **Properties**.
 - c. Select the **Capacity** tab.

If your system usage is greater than your threshold, mail might stop working.
7. Verify that e-mail splitting is disabled.
 - a. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. Double-click **POP**. The POP Properties dialog appears.
 - c. Click the **Configuration** tab.
 - d. For the **Message Split Size** field, verify **No maximum** is selected.
8. Run the Trace TCP/IP Applications command. In the character-based interface, type TRCTCPAPP.
9. Check component journals to locate the problem.

Related concepts

"Controlling e-mail access" on page 10

You need to control who accesses your system through e-mail to protect your data from malicious attacks.

Independent disk pool examples

"Controlling Post Office Protocol access" on page 11

To ensure the security of your system, you need to control Post Office Protocol (POP) access.

"Solving problems with the QtmmSendMail API" on page 48

You can use this troubleshooting process to resolve problems with the Send MIME Mail (QtmmSendMail) API.

Related tasks

"Checking e-mail servers" on page 34

One of the most common problems with e-mail is that the proper servers are not started. Before using your e-mail servers, you need to verify the status of e-mail servers and make sure that they are all running.

"Configuring TCP/IP for e-mail" on page 14

You need to set up TCP/IP before you can configure e-mail on your system.

"Checking mail server framework jobs" on page 49

You should check mail server framework jobs in the QSYSWRK system to determine a possible cause of the error in the QtmmSendMail API.

"Checking component journals" on page 47

You can check journals that record errors to determine how to solve a particular e-mail problem.

"Tracking undelivered e-mail" on page 47

You can use a generic user ID to track problems with undeliverable e-mail. This method can be useful for both e-mail delivery and configuration problems.

Related information

Checking component journals

You can check journals that record errors to determine how to solve a particular e-mail problem.

Your operating system uses various queues, programs, and journaling documents so you can tell why your e-mail server is not delivering your mail. The journaling function can be helpful in offering insight as to what might be going wrong with your e-mail system. Journaling uses processing unit cycles, so the machine performs best when journaling is off.

The journaling function documents the following items:

- Transitions -- programs to queues, queues to program.
- Events -- Arrival of mail through the server, delivery of mail through the client, storage of mail on retry queues or resource busy queues.
- Tracking and some measurement data -- 822 message ID, MSF message ID, size of message, originator, recipients.

Journal records are stored in journal receivers. These receivers are user managed. When the journal becomes full, issue the Change Journal (CHGJRN) command to change to a new journal receiver. The new SMTP Journaling function uses the QZMF journal.

To turn on journaling and view the journal contents, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Double-click **SMTP**.
3. Click the **General** tab.
4. Select the **Enable journal entries** check box.
5. Open an emulation session.
6. To convert the SMTP journal entries to a viewable form, in the character-based interface, type: `DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(jrnlib/zmfstuff) OUTMBR(MAR2) ENDTALEN(512)`, where *jrnlib* is the name of the library, and *zmfstuff* is the name of the physical file.
7. To view the SMTP journal entries, type `DSPPFM FILE(jrnlib/zmfstuff) MBR(MAR2)` on the command line.
8. Press F20 (Shift + F8) to see the journal-specific information.

Related concepts

"Determining problems with e-mail" on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Related reference

"Mail server journal entries" on page 39

Use this information to help you understand the codes and messages used in journal entries.

Tracking undelivered e-mail

You can use a generic user ID to track problems with undeliverable e-mail. This method can be useful for both e-mail delivery and configuration problems.

1. Select or create a user ID to receive notification. In the character-based interface, type CRTUSRPRF (the Create User Profile command) and press Enter.
2. Type WRKDIRE (the Work with Directory Entries command) and press Enter.
3. Type 1 to add the user to the system distribution directory.
4. Ensure that the Mail Store value is 2 and the Preferred Address value is 3.
5. Press F19 (Add Name for SMTP).

6. Type NONDELIVERY@localhost.domain as the SMTP address for any POP user.

This user receives a copy of the undeliverable e-mail.

Note: The user ID you enter must be an actual ID so that it can effectively monitor nondelivery notices. The sender receives a copy of the nondelivery notice with a list of the recipients who did not receive the e-mail.

Related concepts

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Solving problems with the QtmmSendMail API

You can use this troubleshooting process to resolve problems with the Send MIME Mail (QtmmSendMail) API.

- | You might encounter errors that are returned with the QtmmSendMail API. For descriptions of error
- | messages that are returned by the API, refer to the QtmmSendMail API.

Related concepts

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Related reference

Send MIME Mail (QtmmSendMail) API

Checking the API call

To recover from an error with the QtmmSendMail Application Programming Interface (API), you should ensure that you are receiving error messages from the API on your workstation display.

If you code to return the error, then the program returns it to the program. However, if you set this value to 0, as shown in the following examples, then the error appears on your workstation display.

C example

```
Qus_EC_t      Snd_Error_Code;  
Snd_Error_Code.Bytes_Provided=0;
```

RPG example

```
DAPIError    DS  
D APIBytes    1      4B 0  
D CPFId       9      15  
C              Eval  APIBytes    = 0
```

Checking the Multipurpose Internet Mail Extension file

You might have problems with the Multipurpose Internet Mail Extension (MIME) file that is causing the QtmmSendMail API to return an error. You should check the MIME file to ensure that these problems are fixed.

1. Check the MIME file placement. The MIME file must be in the ROOT system and start with a "/", for example, /myfile.txt, and the file name must include the path /mydirectory/myfile.mime.
2. Check the authority levels. QMSF and QTCP profiles must have the authority to read and delete the MIME file.
 - a. In the character-based interface, type WRKLNK (the Work with Object Links command).
 - b. Type 9 (Display) to work with the QMST and QTCP authorities. The Work with Authority display appears.
3. Ensure that the MIME file has an end-of-header (CRLF) statement between the header and the body.

4. Ensure that the MIME file is compliant with MIME Request for Comments (RFCs).

Note: See section 2.1 in RFC2822 (<http://rfc.net/rfc2822.html>) for more information about the end-of-header statement.

Checking mail server framework jobs

You should check mail server framework jobs in the QSYSWRK system to determine a possible cause of the error in the QtmmSendMail API.

1. If the MSF stopped processing the message, check the MSF jobs for error messages.
2. If the framework job completed, the MIME file should be deleted. This means that the framework processed the MIME file. Your problem is not with the API, but in your SMTP configuration.

Related concepts

“Determining problems with e-mail” on page 45

You can use simple steps to determine what is causing a problem with e-mail.

Related information for E-mail



Product manuals, IBM Redbooks publications, Web sites, and other information center topic collections contain information that relates to the E-mail topic collection. You can view or print any of the PDF files.

Manuals






AnyMail/400 Mail Server Framework Support  (about 622 KB)

Read about the framework that drives the i5/OS mail server.

IBM Redbooks

- AS/400® Electronic-Mail Capabilities  (about 3593 KB)
View this popular IBM Redbooks documentation for in-depth information about e-mail and SMTP.
- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet  (about 2160 KB)
This Redbooks documentation provides security information, including steps for cleaning up your i5/OS operating system if your system is the victim of a overwhelming attack.

Web sites

- Support for IBM System i 
Download current PDFs for your i5/OS operating system by using your workstation as a gateway to the Internet PTF page, or view i5/OS solutions from the Technical Information and Databases category.
- RFC Index 
The e-mail protocols are defined in RFCs (Request for Comments). RFCs are the vehicles that are used to define evolving Internet standards. For additional information about SMTP, refer to RFC 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), and RFC 2595 (Using TLS with IMAP, POP3 and ACAP).
- Lotus Domino for i5/OS 
The Web page introduces Lotus Domino for i5/OS and the solutions the licensed program provides.
- Lotus Domino Reference Library 
Learn about Domino by reading the white papers, books, presentations, and more.
- Lotus Documentation 

The Lotus documentation pages provide links to resources, such as product documentation, white papers, Redbooks publications, and more.

Other information

System i and Internet security

See this information center topic collection to secure your System i network.

Related reference

“PDF file for E-mail” on page 1

You can view and print a PDF file of this information.

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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
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 106-0032, 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 YBWA
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 document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, 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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

This E-mail publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

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

AIX
AS/400
Domino
eServer
i5/OS
IBM
IBM (logo)
Infoprint
iSeries
Lotus
Lotus Notes
Redbooks
System i
The Output of e-business
Tivoli

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds 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.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

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, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA