Enter the name of the destination queue. The computer that sends the test message is the computer you selected before clicking **Send Test Message** on the **Tools** menu.

You can send test messages only to test queues. All test queues have a type ID of {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}. To send a test message to a new test queue, click **New Queue**. To send test messages to an existing queue, use MSMQ Explorer to change the queue's type ID to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}.

If you change the type ID of a transactional queue to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}, and send test messages to the transactional queue, the messages are not delivered. Only transactional messages can be sent to transactional queues, and MSMQ Explorer test messages are not transactional. Similarly, if you change the type ID of any queue requiring authentication to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}, and send test messages to the queue, the messages are not delivered (unless the target queue is located on the sending computer).

Click this to send a test message. To send multiple messages to the same queue, click **Send** multiple times.

Click this to close the dialog box.

Click this to create a test queue that can receive test messages. All test queues have a type ID of {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}.

To send test messages to an existing queue, use MSMQ Explorer to change the queue's type ID to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}.

If you change the type ID of a transactional queue to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}, and send test messages to the transactional queue, the messages are not delivered. Only transactional messages can be sent to transactional queues, and MSMQ Explorer test messages are not transactional. Similarly, if you change the type ID of any queue requiring authentication to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}, and send test messages to the queue, the messages are not delivered (unless the target queue is located on the sending computer).

Enter the name of the independent client’s MSMQ in-routing server (InRS). MSMQ routing servers, BSCs, PSCs, and the PEC can be used as InRSs.

If an independent client is configured to use an InRS, every message sent to the independent client is routed through the InRS. However, when an independent client is moved to another site, any InRS and out-routing server (OutRS) settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Click this to delete the selected object.

Click this to delete all selected objects.

Click this to not delete the selected object.

Click this to cancel the deletion of all selected objects.

Type the pathname of the queue to create.

The pathname must be in the computer\queue format, for example, joeuser1\stockquotes.

Select this check box to prevent MSMQ Explorer from warning you about replication delays each time you change replicated information.

Type the name of the public queue you are creating.

Select this check box to create a transactional queue.

Only transactional messages can be sent to transactional queues. Non-transactional messages cannot be sent to transactional queues, and transactional messages cannot be sent to non-transactional queues.

For more information about transactional messaging, see “Transactional Messaging” in Chapter 1 of the “MSMQ Administrator’s Guide.”

Displays the description of the selected event.

Type the name of the CN you want to create.

A connected network (CN) is a collection of computers where any two computers can communicate directly. The two computers must use the same protocol and must be able to establish a session. A computer can belong to multiple CNs, and CNs can span sites.

When you define a CN, you are defining a label. CNs form logical groupings of computers that can communicate directly.

Enter the protocol you want to pair with the specified CN. If you are pairing a protocol with a foreign computer, click **Foreign**.

A foreign computer does not run MSMQ, but can exchange messages with MSMQ through an MSMQ connector server. A foreign computer must be a member of at least one foreign CN.

Type the name of the site to be paired with **Cost**. This creates a new site-link cost between the specified site and the site for which you are setting properties.

Site-link costs can be defined using relative numbers between 0 and 999,999. You must define the relative cost of routing between sites by balancing cost with delay (the speed of one link versus another). A site-link cost of zero indicates that the two sites are not connected.

Type the site-link cost you want to pair with the specified site.

Site-link costs can be defined using relative numbers between 0 and 999,999. You must define the relative cost of routing among sites by balancing cost with delay (the speed of one link versus another). A site-link cost of zero indicates that the two sites are not connected.

Type a new name for the enterprise or site.

Click this to set access permissions for the selected enterprise, site, CN, computer, or queue.

Click this to set auditing settings for the selected enterprise, site, CN, computer, or queue.

Click this to take ownership of the selected enterprise, site, CN, computer, or queue.

When you take ownership of an object, you control how permissions are set on the object. To take ownership of an object, you must have the Take Ownership permission for that object. By default, only those users that have Full Control permissions for an object have the Take Ownership permission.

Click this to move a column name from **Available Columns** to **Show the following**.

Click this to move a column name from **Show the following** to **Available Columns**.

Select a column name in **Show the following** and click this button to move the column’s display location one column to the left. MSMQ Explorer displays the columns from left to right, based on the order of the column names in **Show the following**.

Select a column name in **Show the following** and click this button to move the column’s display location one column to the right. MSMQ Explorer displays the columns from left to right, based on the order of the column names in **Show the following**.

Click this to add CN/network address pairs.

Click this to edit existing CN/network address pairs

Click this to remove existing CN/network address pairs

Displays the CNs used by this computer. This also displays the network addresses that are paired with the CNs.

Displays the selected MSMQ in-routing servers (InRSs) for the selected independent client.

If an independent client is configured to use an InRS, every message sent to the independent client is routed through the InRS. However, when an independent client is moved to another site, any InRS and out-routing server (OutRS) settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Click this to configure the independent client to use one or more MSMQ in-routing servers (InRS).

If an independent client is configured to use an InRS, every message sent to the independent client is routed through the InRS. However, when an independent client is moved to another site, any InRS and out-routing server (OutRS) settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Click this to configure the independent client’s existing MSMQ in-routing server (InRS) settings.

If an independent client is configured to use an InRS, every message sent to the independent client is routed through the InRS. However, when an independent client is moved to another site, any InRS and out-routing server (OutRS) settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Select one or more MSMQ in-routing servers (InRSs) and then click this button to discontinue the independent client’s use of selected InRSs.

If an independent client is configured to use an InRS, every message sent to the independent client is routed through the InRS. However, when an independent client is moved to another site, any InRS and out-routing server (OutRS) settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Lists the selected MSMQ out-routing servers (OutRSs) for the selected independent client.

If an independent client is configured to use an OutRS, every outgoing message is routed from the independent client to the OutRS. However, when an independent client is moved to another site, any in-routing server (InRS) and OutRS settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Click this to configure the independent client to use one or more out-routing servers (OutRSs).

If an independent client is configured to use an OutRS, every outgoing message is routed from the independent client to the OutRS. However, when an independent client is moved to another site, any in-routing server (InRS) and OutRS settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Click this to configure the independent client’s existing out-routing server (OutRS) settings.

If an independent client is configured to use an OutRS, every outgoing message is routed from the independent client to the OutRS. However, when an independent client is moved to another site, any in-routing server (InRS) and OutRS settings are disabled until the independent client returns to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Select one or more out-routing servers (OutRSs) and then click this button to discontinue the independent client’s use of selected OutRSs.

If an independent client is configured to use an OutRS, every outgoing message is routed from the independent client to the OutRS. However, when an independent client is moved to another site, any in-routing server (InRS) and OutRS settings are disabled until the independent client is returned to its original site.

InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ routing server can be used as an independent client’s InRS and OutRS.

Displays the site’s current site links.

Site-link costs can be defined using relative numbers between 0 and 999,999. You must define the relative cost of routing among sites by balancing cost with delay (the speed of one link versus another). A site-link cost of zero indicates that the two sites are not connected.

Click this to remove existing site links.

Displays the site’s current site gates.

If a site is configured to use a site gate, every MSMQ message sent between computers in different sites must be routed through the site gate. This is how MSMQ achieves inter-site session concentration.

Click this to configure the site to use one or more site gates.

Click this to configure the site’s existing site gate settings.

Select one or more site gates and then click this button to remove the site gates from the selected sites.

Displays the queue’s label. To change the queue’s label, type a new label in **Label**.

Displays the queue’s type ID. To change the queue’s type ID, type a new type ID in **Type ID**.

The queue’s type ID specifies the type of service provided by the queue. For example, if your application receives messages from a MAPI application, it requires an input queue with a specific MAPI type-ID. You can also use the queue type-ID to search for, open, or delete a specific type of queue.

Type the total size of all messages that can be stored in the queue.

When the queue quota you specify is reached, messages cannot be sent to the queue until the cumulative size of messages in the queue drops below the queue quota.

Indicates whether the queue will accept only transactional messages.

This option is always unavailable because it cannot be changed from MSMQ Explorer.

Select this check box to enable target journaling for the queue.

Target journaling is the process of storing a copy of all incoming messages. When target journaling is enabled, a copy of each incoming message is placed in the target-journal queue when the message is removed (read) from the target queue. The target-journal queue (called Journal) is created for each queue when the queue is created. MSMQ Explorer displays each queue’s target-journal queue under each public queue.

When you enable target journaling, only messages that are sent after the change are put in the journal queue.

Type the total size of all messages that can be stored in the queue’s journal queue. When the target journal queue quota is reached, target journaling ceases.

Enter the privacy level required by the queue. If the privacy level is **None**, the queue accepts only unencrypted messages. If the privacy level is **Optional**, the queue accepts both unencrypted and encrypted messages. If the privacy level is **Body**, the queue accepts only encrypted messages.

Click this to refresh the event display.

When you click **Refresh**, MSMQ reads the Windows NT application log and displays all MSMQ events.

Click this to run Windows NT Event Viewer.

Displays all MSMQ events from the Windows NT application log.

Type, in seconds, how often MQIS information is replicated between the selected site controller and other site controllers.

When you specify the MQIS defaults for the enterprise, you specify what the default MQIS replication intervals are for all new sites. When you specify the MQIS replication intervals for a specific site, you specify how often that specific site controller sends its replicated information to other site controllers.

For information on MQIS replication and ownership, see Chapter 1 of the “MSMQ Administrator’s Guide.”

Type, in seconds, how often MQIS information is replicated between the selected site's PEC or between the PSC and the site's BSCs.

When you specify the MQIS defaults for the enterprise, you specify what the default MQIS replication intervals are for all new sites. When you specify the MQIS replication intervals for a specific site, you specify how often that specific site controller sends its replicated information to other site controllers.

For information on MQIS replication and ownership, see Chapter 1 of the "MSMQ Administrator's Guide."

Type the complete name of the computer for which you want to search. You cannot use wildcards or specify a partial computer name.

Enter the type of computer for which you want to search. You can search for all computers, MSMQ routing servers, BSCs, and PSCs (including the PEC).

MSMQ Explorer does not display MSMQ dependent clients or RAS connectivity servers because they do not run the MSMQ service.

Type the complete name of the queue for which you want to search. You cannot use wildcards or specify a partial queue name.

Type the complete GUID of the queue for which you want to search. You cannot use wildcards or specify a partial GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Click this to create a new queue for receiving message route-tracking messages.

Select this check box to have MSMQ track all messages sent from the selected computer.

When message route tracking is enabled for a computer, all messages sent from the computer are tracked as they traverse the MSMQ network, even if the MSMQ-based application does not set the message route tracking property. As each message passes through an MSMQ routing server, a message is sent to the report queue, indicating which server the message passed through.

After message route tracking is enabled, you can use MSMQ Explorer to send test messages and view the contents of the report queue.

Select this check box to have MSMQ track only test messages sent from the selected computer.

Type, in seconds, how often MSMQ should refresh the display of MSMQ performance counters for the selected computer or queue. The higher the refresh rate, the more system resources are used for monitoring overhead.

Click this to refresh the display of MSMQ performance counters for the selected computer or queue.

Click this to run Windows NT Performance Monitor. From Performance Monitor you can configure the display of MSMQ performance counters. The MSMQ performance counters are grouped under four objects: MSMQ IS, MSMQ QM, MSMQ Queue, and MSMQ Session.

For more information on MSMQ performance counters, see Chapter 4 of the “MSMQ Administrator’s Guide.”

Displays some of the available MSMQ performance counters for the selected computer or queue. You can run Windows NT Performance Monitor to see all of the available MSMQ performance counters. The MSMQ performance counters are grouped under four objects: MSMQ IS, MSMQ QM, MSMQ Queue, and MSMQ Session. For an explanation of each counter, click **Explain**.

Displays the message’s label.

The message label is defined by the sending application.

Displays the message’s GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the message’s priority.

MSMQ routes and delivers messages based on a combination of queue priority, called the *base priority*, and message priority. Messages are routed and delivered queue by priority first, and then by message priority. The queue priority can be set from -32768 to 32767; the default is 0. MSMQ-based applications can send messages with a priority of 0 through 7, with 7 as the highest priority.

Displays the computer’s NetBIOS computer name.

Displays the site to which the computer currently belongs.

Displays the computer’s GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the name of the site.

To change the site’s name, right-click the site in MSMQ Explorer, and then click **Rename**.

Displays the site’s GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the queue’s pathname.

The queue pathname is a combination of queue name and the name of the computer on which the queue was created. Queue pathnames are always unique in an enterprise.

Displays the date that the queue was created.

Displays the date that the queue was last modified.

Displays the CN name.

To change the CN name or the protocol associated with the CN, right-click the PEC, click **Properties**, and then click the **Network** tab.

Displays the protocol associated with the CN.

To change the CN name or the protocol associated with the CN, right-click the PEC, click **Properties**, and then click the **Network** tab.

Displays the CN’s GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the enterprise name. You can change the enterprise name by right-clicking the enterprise in MSMQ Explorer and then clicking **Rename**.

Displays the NetBIOS name of the PEC.

Displays the site or enterprise name.

Enter the network address you want to pair with the selected connected network (CN).

A CN is a collection of computers in which any two computers can communicate directly. The two computers must use the same protocol and must be able to establish a session. A computer can belong to multiple CNs and CNs can span sites.

Enter the CN you want to pair with the selected network address.

Displays the date and time the computer joined the enterprise.

Displays the date and time the computer properties were last modified.

Displays the message class.

The message class indicates message type. A message can be a normal MSMQ message, a positive or negative acknowledgment message, or a report message. This property is set by MSMQ. All messages created by MSMQ-based applications are normal messages.

Displays **Yes** or **No**, indicating whether message route tracking is enabled for the message.

Displays the CNs that the foreign computer does not belong to.

Displays the CNs that the foreign computer will belong to after you click **OK**.

Click this to add the CN to the list of CNs under **Member of**.

Click this to remove the CN from the list of CNs under **Member of**.

Displays the format name of the message’s queue.

Displays the pathname of the message’s queue.

Displays the format name of the message’s response queue.

Displays the pathname of the message’s response queue.

Displays the format name of the message’s administration queue.

Displays the pathname of the message’s administration queue.

Displays the GUID of the computer that sent the message.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the pathname of the computer that sent the message.

Displays **Yes** or **No**, indicating whether the message is authenticated.

Displays the hashing algorithm. The hashing algorithm values are defined by the sending application.

Displays **Yes** or **No**, indicating whether the message is encrypted.

Displays the name of the encryption algorithm used by the sending application. This algorithm encrypts the message body. The two possible encryption values are RC2 and RC4. If the message is not encrypted, nothing is displayed.

Type the total size, in kilobytes, of all messages that can be stored in all queues on the selected computer.

When the computer quota is reached, messages cannot be sent to any queues on the computer until the cumulative size of messages in the queues drops below the queue quota.

Type the total size, in kilobytes, of all messages that can be stored in the selected computer’s source-journal queue.

When the source-journal queue quota is reached, source journaling ceases until the cumulative size of messages drops below the quota.

Select this check box to specify the queue quota for the selected queue.

When the queue quota is reached, messages cannot be sent to the queue until the cumulative size of messages in the queue drops below the queue quota.

Select this check box to specify the target-journal queue quota for the selected queue’s journal queue. When the target-journal queue quota is reached, target journaling ceases.

Select this check box to specify the computer quota for the selected computer.

When the computer quota is reached, messages cannot be sent to the any queues on the computer until the cumulative size of messages in all queues on the computer drops below the computer quota.

Select this check box to specify the source-journal quota for the selected computer’s source-journal queue.

Source journaling is the process of storing a copy of an outgoing message. Source journaling is configured on a message basis, and is therefore a property set by the sending application. When source journaling is enabled for a message, a copy of the message is put in the source-journal queue of the sending computer when the message arrives at the target queue. When the source-journal queue quota is reached, source journaling ceases.

In MSMQ Explorer, the source-journal queue is displayed underneath the computer.

Displays the computer’s function. The computer can be a PEC, PSC, BSC, MSMQ routing server, or independent client.

Select this check box to specify that the queue will accept only authenticated messages.

Enter the base priority of the queue.

MSMQ routes and delivers messages based on a combination of queue priority, called the *base priority*, and message priority. Messages are routed and delivered by queue priority first, and then by message priority. Queue priority for a public queue can be set by any MSMQ-based application with write permissions for the queue. The priority can be set any time. The queue priority can be set from -32768 to 32767. The default priority for public queues is 0. Private queues do not support queue priority.

Displays the date and time the message was sent. Although MSMQ stores message time using universal time, the time MSMQ Explorer displays is adjusted for your current time zone.

Displays the date and time the message was received. Although MSMQ stores message time using universal time, the time MSMQ Explorer displays is adjusted for your current time zone.

Type the name of the foreign computer you are creating.

A foreign computer is a computer that does not run MSMQ, but can exchange messages with MSMQ through an MSMQ connector server. A foreign computer must be a member of at least one foreign CN.

Type, in seconds, how often MQIS information is replicated between a site controller and other site controllers and between a site controller and its BSCs.

When you specify the MQIS defaults for the enterprise, you specify the default MQIS replication intervals for all new sites. When you specify the MQIS replication intervals for a specific site, you specify how often that specific site controller sends its replicated information to other site controllers.

For information on MQIS replication and ownership, see Chapter 1 of the “MSMQ Administrator’s Guide.”

Enter the default maximum time for a message to reach its destination queue.

Enter how long, in hours or days, a message can take to reach its destination queue before being placed in a dead letter queue. This value is called time-to-reach-queue. The default is 90 days.

Messages are placed in a dead letter queue only if the sending application set the appropriate message property.

Enter the units of measure you want to use with the associated **Default lifetime of a message in the network** value. You can specify this value in days or hours.

Displays the number of test messages you sent.

Displays the columns that do not display in the right pane of MSMQ Explorer. To configure MSMQ Explorer to display a column, click the column name and then click **Add**.

For more information on data displayed under each column heading, in MSMQ Explorer, click the **Help** menu, click **Help Topics**, click the **Index** tab, and then select the MSMQ Explorer Columns help topic for the object you want.

Displays the columns that display in the right pane of MSMQ Explorer. To configure MSMQ Explorer to stop displaying a column, click the column name and then click **Remove**.

For more information on data displayed under each column heading, in MSMQ Explorer, click the **Help** menu, click **Help Topics**, click the **Index** tab, and then select the MSMQ Explorer Columns help topic for the object you want.

Displays the message body contents. If the message body contains text data, this information is readable. If the message body contains binary information, this dialog box displays hexadecimal data along with its text translation.

If the body of the message contains Unicode characters, the message text is readable if the **Body** column is displayed when you select a queue (MSMQ Explorer does not display the **Body** column by default). However, the message body is not readable when you view the **Body** properties for the message. When you view the message properties, Unicode characters are displayed as 2-byte values.

Displays the format name and pathname of the message’s queue.

Displays the format name and pathname of the message’s response queue.

Displays the format name and pathname of the message’s administration queue.

Displays the name of the user who sent the message.

Displays the security identifier (SID) of the user who sent the message.

Click this to change settings for existing site links.

Click this to establish one or more site links.

Select this check box to enable target journaling for the selected queue.

Select the **Limit journal storage (in K) to** check box to specify the target-journal queue quota for the selected queue.

Target journaling is the process of storing a copy of all incoming messages. When target journaling is enabled, a copy of each incoming message is placed in the target-journal queue when the message is removed (read) from the target queue. The target journal queue (called Journal) is created for each queue when the queue is created. MSMQ Explorer displays each queue’s target-journal queue underneath the queue.

Displays the GUID and pathname of the computer that sent the message.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

User and **SID** display the name (in domain name\user name format) and the SID of the user logged on at the source computer. If the sender was logged on to a Windows NT Server domain when the message was sent, MSMQ Explorer displays **Unknown user** (except on the computer that sent the message — in this case, the user name is available).

Authenticated displays **Yes** or **No**, indicating whether the message is authenticated.

Hash Algorithm displays the hashing algorithm used for the message digest. The hashing algorithm values are defined by the sending application.

Displays **Yes** or **No**, indicating whether the message is encrypted. If the message is encrypted, this displays the name of the encryption algorithm used by the sending application. The two possible encryption values are RC2 and RC4. If the message is not encrypted, nothing is displayed.

Displays when MSMQ cannot communicate with the selected computer. The computer may be offline or a network link may broken.

Displays the name of the site in which the computer was originally installed.

You can use message route tracking to track the path messages take on your MSMQ network. As the messages pass through an MSMQ routing server, a message is sent to the report queue indicating which server the message passed through.

Enabling message route tracking is a two step process. First, you must enable message route tracking by defining a report queue for the sending computer. Second, the application must set the correct message property. The application developer must set this property, or enable some way for it to be set by the user (for example, through the Windows registry), so that message route tracking can be enabled for the application.

Because all test messages are sent with message route tracking enabled, if the sending computer has a report queue, the message path is tracked because all test messages are sent with message route tracking enabled.

Enter the pathname of the report queue.

Message route tracking is used to track the path messages take as they traverse your MSMQ network. As the messages pass through an MSMQ routing server, a message is sent to the report queue indicating which server the message passed through. You can track message routes for applications or only track test messages. To track message routes for applications, select **Track all messages** and set the message route tracking flag within the sending application.

Displays the queue’s GUID.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer. The GUID format is {12345678-1234-1234-1234-123456789012}.

Click this to refresh the display of dependent clients that use the selected MSMQ server as their supporting server.

Displays the dependent clients that use the selected MSMQ server as their supporting server. Dependent clients are displayed here if there is an MSMQ-based application running on the client that has at least one open queue handle.

Click a letter to scroll to that section of the glossary, and then click on the term you would like defined.

A

- ActiveX controls
- administration queue
- API
- authentication

B

- Backup Site Controller
- base priority
- BSC

C

- connector queue
- controller server
- computer pathname
- computer quota
- computer ID
- CN
- connected network
- CSP

D

- dead letter queue
- destination queue

E

- encryption
- enterprise network
- express message

F

- foreign computer
- foreign CN
- format name

G

- GUID

H

- hash algorithm
- hop

I

- in-routing server
- information server
- information store
- InRS
- inter-site routing
- intra-site routing
- ISV

J

- journaling

- journal queue
- journal quota

K

There are no glossary entries for this section.

L

There are no glossary entries for this section.

M

- message
- message class
- message label
- Microsoft Message Queue Service
- MQIS
- MS DTC
- MSMQ
- MSMQ connector server
- MSMQ dependent client
- MSMQ independent client
- MSMQ RAS connectivity service
- MSMQ routing server
- MSMQ service
- MSMQ server

N

- non-repudiation

O

- out-routing server
- OutRS

P

- PEC
- permission
- primary enterprise controller
- primary site controller
- privacy level
- private queues
- PSC
- public queues

Q

- QM
- queue manager
- queue pathname
- queue quota
- queue type

R

- recoverable message
- report queue
- resource manager
- response queue
- right
- routing
- RSA

S

- site pathname

- SDK
- sender ID
- session
- session concentration
- site
- site controller server
- site gate
- site link
- site-link cost
- source journaling
- source computer
- supporting server

T

- target journaling
- transaction
- transaction dead letter queue
- type ID

U

There are no glossary entries for this section.

V

There are no glossary entries for this section.

W

There are no glossary entries for this section.

X

There are no glossary entries for this section.

Y

There are no glossary entries for this section.

Z

There are no glossary entries for this section.

ActiveX controls

You can use the ActiveX controls provided by MSMQ and Visual Basic (VB) or any other ActiveX container application (such as Microsoft Access) to quickly and easily write MSMQ-based applications.

administration queue

MSMQ uses administration queues to pass acknowledgment messages. Acknowledgment messages, generated by MSMQ, are used by the application that sent the original message. These messages indicate that the original messages either arrived (a positive acknowledgment) or that an error occurred before the original message could be retrieved (a negative acknowledgment). A positive acknowledgment message can also indicate whether the original message was retrieved by the target application. A negative acknowledgment message can also indicate why the original message was not received or retrieved.

The application programmer determines whether to use acknowledgments. If acknowledgments are used, the application programmer must specify an administration queue in the source application and the type of acknowledgment messages to send to the queue.

API

Application programming interface.

authentication

Authentication (also called signing) is the process of verifying that the message sender is authentic (that is, that the sender is not being impersonated by another user). MSMQ uses digital signatures (commonly called certificates) to provide message authentication.

Class 1 or Class 2 digital signatures must be obtained from a cryptographic service provider (CSP), such as AT&T or Verisign. The CSP does not have to provide full *RSA* support, only a signing. Any signing CSP can be used as long as it is installed on both the sending and receiving computers. To use non-internal certificates the computer must have Microsoft® Internet Explorer version 3.0 installed.

backup site controller

Sites do not require backup site controllers (BSCs). However, one or more BSCs can be installed at each site to provide load balancing and failure recovery, should the PSC or PEC fail. The BSC holds a read-only replica of the PSC or PEC MQIS database and also functions as an MSMQ routing server.

For information on the MQIS database and replication, see the *Microsoft Message Queue Server Administrator's Guide*, Chapter 1, "Understanding MSMQ."

base priority

The base priority of a public queue specifies the queue's priority. The base priority can be set by any MSMQ-based application with write permissions for the queue. The base priority can be set any time. The public queue priority can be set from -32768 to 32767 (the default priority is 0). Private queues do not support queue priority.

MSMQ routes and delivers messages based on a combination of queue priority and message priority. Messages are routed and delivered by queue priority first, and by message priority second.

BSC

See *backup site controller*.

computer ID

A GUID created by MSMQ when the computer joins the enterprise.

computer pathname

The same as the computer name.

computer quota

Specifies the cumulative limit for message size on a computer, based on the total size of the messages. The computer quota can be set independently of the queue quota. When a computer quota is reached, messages can no longer be sent to the computer until one or more messages are removed from queues.

MSMQ enforces the computer limit no matter how many queues are opened or what the cumulative queue quotas are. For example, if you specify a 10 MB limit for each of the six public queues on a computer and a 50 MB total limit for a computer, MSMQ enforces the 50 MB computer limit even if no queue has reached its 10 MB queue-quota limit. However, each queue quota still prevents any single queue from storing more than 10 MB of messages.

connector queue

Created on MSMQ connector servers. You can use the MSMQ connector server to exchange messages with computers that are not running MSMQ (called foreign computers). The user account running the MSMQ connector must have the Open Connector permission on the foreign CN to open a connector queue.

controller server

Refers to PECs, PSCs, and BSCs. *Site controller server* refers to just the enterprise PEC and any PSCs.

CN

Connected network. See *connected network* for more information.

connected network

A collection of computers in which any two computers can communicate directly.

CSP

Cryptographic service provider. CSPs provide digital signatures for authenticating messages. For more information, see *authentication*.

dead letter queue

A queue in which MSMQ stores undeliverable messages. Each computer has a dead letter queue.

destination queue

Messages are sent from source computers to destination queues. As they traverse your MSMQ network, the messages may pass through intermediary store-and-forward servers.

encryption

The process of coding and decoding messages, ensuring they cannot be read or used by anyone not authorized to read or use the message. MSMQ supports encryption through the use of public and private keys.

The MSMQ public key implementation is based on the Microsoft CryptoAPI, and uses the Microsoft Base Cryptographic Provider version 1.0.

enterprise network

A collection of sites connected through slow and expensive links.

express message

MSMQ supports two delivery methods: express and recoverable. Choosing between express and recoverable delivery is a matter of trading performance and resource use for reliability and failure recovery. In general, express messages use fewer resources and are faster than recoverable messages. However, express messages cannot be recovered if the computer storing the memory-mapped message files fails. Recoverable messages use more resources and are slower than express messages, but can be recovered no matter which computer fails.

foreign computer

A computer that does not run MSMQ but can exchange messages with MSMQ through an MSMQ connector server.

foreign CN

A CN that contains foreign computers (computers that do not run MSMQ) and an MSMQ connector server (a computer that handles messaging between your MSMQ enterprise and other message queuing systems).

format name

A representation of the queue used by the MSMQ API. Format names are used to specify a queue when making calls to several API functions.

GUID

A globally unique identifier (GUID) is a 128-bit (16-byte) integer that an algorithm creates. The algorithm uses several criteria, including the current date, time, and a computer identifier, to ensure that it is unique. The GUID format is {12345678-1234-1234-1234-123456789012}.

MSMQ uses GUIDs to represent the ID of many objects, including computers, queues, and messages.

hash algorithm

The hashing algorithm used in encrypting messages.

hop

A unit of measurement used in intra-site routing. Each MSMQ routing server through which a message must pass adds one to the number of hops the message travels. If the message travels directly between two computers that establish a session, the message travels only one hop.

in-routing server

An MSMQ routing server that provides session concentration by acting as a gateway for all incoming messages for one or more independent clients. MSMQ independent clients can be configured to use InRSs, OutRSs, or both.

information server

See *controller server*.

information store

See *MQIS*.

InRS

See *in-routing server*.

inter-site routing

The process of routing messages between sites.

intra-site routing

The process of routing messages within a site.

ISV

Independent software vendor.

journaling

The process of logging or storing messages in a queue. See *journal queue*.

journal queue

The process of logging or storing a copy of a message in a queue. Journal messages are stored in a queue called Journal.

Two types of journaling are available: source and target. Source journaling is the process of storing a copy of an outgoing message. It is configured on a message basis and is, therefore, a property set by the sending application. When journaling is enabled for a message, a copy of the message is placed in the source journal queue on the source computer when the message is queued. In MSMQ Explorer, the source journal queue is displayed under the computer.

Target journaling is the process of storing a copy of incoming messages. It is configured on a queue basis. When target journaling is enabled, a copy of each incoming message is placed in the target journal queue when the message is removed (read) from the target queue. A target journal queue (simply called Journal) is created for each queue when the queue is created. In MSMQ Explorer, target journal queues are displayed under each public queue.

journal quota

Specifies the cumulative limit for messages in the journal queue. The limit is based on cumulative message size. When a journal queue’s quota is reached, messages are no longer journaled.

message

A unit of information or data sent between computers. The message can contain text or binary data as defined by the sending application. Messages can be up to 4 MB in size.

message class

Indicates the message source and its use. A message class can be normal, a positive or negative acknowledgment message, or a report message. This property is set by MSMQ or an MSMQ connector application. All messages created by MSMQ-based applications are normal messages.

message label

A string defined by the sending application. The label can be viewed from MSMQ Explorer and is never encrypted.

Microsoft Message Queue Service

The MSMQ component that provides the core MSMQ functionality. This service runs on all MSMQ independent clients and servers.

MS DTC

Microsoft Distributed Transaction Coordinator (MS DTC) is a transaction manager that coordinates transactions that span multiple resource managers. Work can be committed as an atomic transaction even if the work spans multiple resource managers, even on separate computers.

MQIS

MSMQ Information Store. The MQIS is a SQL 6.5 replicated database. For information on the MQIS database and replication, see the *Microsoft Message Queue Server Administrator's Guide*, Chapter 1, "Understanding MSMQ."

MSMQ

Microsoft Message Queue Server.

MSMQ dependent client

MSMQ dependent clients function much like MSMQ independent clients. However, they cannot function without synchronous access to an MSMQ server (PEC, PSC, BSC, or MSMQ routing server).

MSMQ dependent clients can be installed on computers running Windows 95 and on Intel-compatible computers running Windows NT Workstation or Windows NT Server. (Alpha and PowerPC computers running Windows NT are not supported).

MSMQ dependent clients require synchronous access to the supporting MSMQ server to perform all standard MSMQ functions, such as creating queues, sending messages, and receiving messages.

MSMQ connector server

MSMQ connector servers enables MSMQ-based applications to communicate with computers, called *foreign computers*, that use other messaging systems. MSMQ connector servers use *foreign CNs* and *connector queues* to communicate with foreign computers. The Level 8 Systems MSMQ message queuing product is an example of an MSMQ connector server.

To develop an MSMQ connector server, you must obtain the MSMQ Connector Software Development Kit (SDK).

MSMQ RAS connectivity service

The MSMQ RAS connectivity service enables MSMQ independent clients to connect to your MSMQ network through a Windows NT Server remote access service (RAS) server. To reduce long distance charges and ensure independent clients always connect to the same site, you should configure your Windows NT RAS servers with the MSMQ RAS connectivity service at each site. Although it is possible to configure MSMQ independent clients to connect to your MSMQ network through a RAS server in any site, this configuration does not provide the same benefits.

MSMQ routing server

Supports dynamic routing and intermediate store-and-forward message queuing. MSMQ routing servers enable computers that use different protocols to communicate. If configured to do so, MSMQ routing servers provide session concentration. Unlike BSCs, MSMQ routing servers do not hold a read-only replica of the PSC or PEC database.

MSMQ service

See *Microsoft Message Queue Service*.

MSMQ server

MSMQ uses four server types to control message queuing:

- Primary enterprise controller (PEC)
- Primary site controller (PSC)
- Backup site controller (BSC)
- MSMQ routing server

Any server can also function as a connector server.

MSMQ independent client

MSMQ independent client software can be installed on computers running Windows 95, Windows NT Workstation version 4.0 or later, or Windows NT Server version 4.0 or later. MSMQ independent clients can create and modify queues, and send and receive messages, just as MSMQ servers can. MSMQ independent clients can create queues and store messages on the local computer, without synchronous access to an MSMQ server. The primary difference between MSMQ independent clients and MSMQ servers is that independent clients do not have the intermediate store-and-forward capability of MSMQ servers, nor do they store information from the distributed MSMQ database.

In addition to the basic MSMQ files, you can install the MSMQ Software Development Kit (SDK) on MSMQ independent clients.

You can also install the MSMQ Explorer on MSMQ independent clients running Windows NT Workstation or Windows NT Server. You can use the MSMQ Explorer to administer your MSMQ enterprise remotely from computers running Windows NT Workstation.

non-repudiation

MSMQ authentication provides non-repudiation (because no user can sign a message with another user’s identity, no user can refute that he or she sent a message if it contains his or her signature).

out-routing server

An MSMQ routing server that provides session concentration by acting as a gateway for all outgoing messages for one or more independent clients. MSMQ independent clients can be configured to use InRSs, OutRSs, or both.

OutRS

See *out-routing server*.

PEC

See *primary enterprise controller*.

permission

A rule associated with an object (such as an enterprise, site, CN, computer, or queue) to regulate which users can access the object and in what manner. Permissions apply to specific objects and are different from rights, which apply to the system as a whole.

primary enterprise controller

The primary enterprise controller (PEC) contains a master copy of the enterprise and site settings in the MQIS database and certification keys (used in authenticating messages). Administrators install one PEC on an MSMQ network. The PEC functions as a PSC for one site and also functions as an MSMQ routing server.

For information on the MQIS database and replication, see the *Microsoft Message Queue Server Administrator's Guide*, Chapter 1, "Understanding MSMQ."

primary site controller

You install one primary site controller (PSC) for each additional site in your MSMQ network—the PEC functions as the site controller for the initial site you create. The PSC stores information about the site's computers and queues in the MQIS, and also functions as an MSMQ routing server.

For information on the MQIS database and replication, see the *Microsoft Message Queue Server Administrator's Guide*, Chapter 1, "Understanding MSMQ."

privacy level

Specifies whether the queue accepts encrypted messages, unencrypted messages, or both. If the privacy level is None, the queue accepts only unencrypted messages. If the privacy level is Optional, the queue accepts both unencrypted and encrypted messages. If the privacy level is Body, the queue accepts only encrypted messages.

private queues

Private queues are not published in the MQIS, and therefore do not add to the MQIS replication load. Private queues can be accessed only by applications that have access to the full format name of the queue. In the default view, MSMQ Explorer does not display private queues.

PSC

See *primary site controller*.

public queues

Published in the MQIS. All public queues are replicated throughout the enterprise and can, therefore, be located by any computer within the enterprise.

QM

See *queue manager*.

queue manager

A component of the Microsoft Message Queue Service.

queue name

User friendly names created on the computer on which the queue resides.

queue pathname

Queues are referenced by the queue pathname. The queue pathname is a combination of the computer name where the queue resides and the queue name. For example, if you create a queue called Myqueue on a computer called Joeuser1, the queue pathname is Joeuser1\Myqueue.

queue quota

Specifies the cumulative limit for messages in public queues. The queue quota limits are based on size and can be set independently of the computer quota. When a queue quota is reached, messages can no longer be sent to the queue until one or more messages are removed from the queue and enough space is available for the message.

queue type

A GUID specified by the application that created the queue. Consistent use of queue type IDs can help MSMQ-based applications locate different types of queues. For example, if your application receives messages from a MAPI application, it can search for an input queue with a specific MAPI type-ID. Your MSMQ-based applications should use a different GUID for each queue type used within your enterprise.

recoverable message

MSMQ supports two delivery methods: express and recoverable. Choosing between express and recoverable delivery is a matter of trading performance and resource use for reliability and failure recovery. In general, express messages use fewer resources and are faster than recoverable messages. However, express messages cannot be recovered if the computer storing the memory-mapped message files fails. Recoverable messages use more resources and are slower than express messages, but can be recovered no matter which computer fails.

report queue

Contains MSMQ-generated report messages that track the route of your application messages as they move toward their target queues. A report message is generated each time a message passes through an MSMQ routing server. Report queues can be used when sending test messages and when tracking message routes for a specific application.

resource manager

A system service that manages durable data. Server applications use resource managers to maintain the durable state of the application, such as the record of inventory on hand, pending orders, and accounts receivable. The resource managers work in cooperation with the transaction manager to provide the application with a guarantee of atomicity and isolation (using the two-phase commit protocol).

For example, both MSMQ and Microsoft SQL Server are resource managers.

response queue

A message property that is set by the sending application and is used by the receiving application for replying to messages. For example, an application might send a response message to a response queue every time the application receives a message.

right

Authorizes a user to perform certain actions on the system. Rights apply to the system as a whole and are different from permissions, which apply to specific objects.

routing

MSMQ establishes a direct connection (a session) using the underlying protocol if possible. When a direct connection is not possible or not allowed, MSMQ uses its own routing system. MSMQ routing occurs when one or more of the following conditions exist.

- A session cannot be established between the sender and the receiver (for example, when the source and target computers do not share a common CN or the target computer is offline)
- In-routing servers (InRSs) or out-routing servers (OutRSs) are defined for the sender or receiver
- Messages must travel between two sites, and one or both sites have a site gate defined

MSMQ servers make two assumptions about your MSMQ network: *Intra-site routing* is fast and inexpensive, while *inter-site routing* is slow and expensive.

RSA

The RSA public-key cipher was developed by (and named after) Ron Rivest, Adi Shamir, and Leonard Adleman in the late 1970’s. This algorithm is well known; you can read about its internal details in any book on cryptography.

RSA is used by many CSPs to encrypt and decrypt keys and to generate and verify digital signatures. This algorithm is used when operations are performed using either the key exchange or digital-signature key pair. When using CryptoAPI, this algorithm cannot be used to encrypt bulk data.

RSA is a variable-key-length cipher. However, when using CryptoAPI with the Microsoft RSA Base Provider, the key length is hard-coded to 512 bits.

site pathname

The name of the site.

SDK

Acronym for Software Development Kit. The MSMQ SDK and related documentation are installed when you click **Development Workstation** or **Development Server** during Setup.

sender ID

Displays the security identifier (SID) of the user who was logged on at the source computer.

session

The time during which two computers maintain a connection and (usually) transfer information.

session concentration

Used to reduce sessions within a site and/or reduce sessions between sites. Unnecessary sessions can increase connection and bandwidth costs. MSMQ session concentration reduces these costs by funneling connections through MSMQ servers.

MSMQ supports two types of session concentration: intra-site and inter-site. Intra-site session concentration typically reduces network bandwidth use within a site. Inter-site session concentration typically reduces the number of sessions between sites.

By loading specific servers with more independent clients, you can manually load or tune your MSMQ network using session concentration. For example, all MSMQ independent clients in one department can be configured to send and receive all messages through a specific server or set of servers.

site

A physical collection of computers where communication between any two computers is fast and inexpensive. Sites usually parallel the physical location of the computers. However, every computer in a site does not necessarily have to run the same protocol. Computers in the same site may not be able to directly communicate with each other.

site controller server

Refers to PECs and PSCs, usually in the context of installing MSMQ. *Controller server* refers to the enterprise PEC, all PSCs, and all BSCs.

site gate

You can establish site gates to provide inter-site session concentration. If a site is configured to use a site gate, every MSMQ message sent between computers in different sites must be routed through the site gate. The routing topology beyond the source site is transparent to the computers within the site, with the exception of the site gate. Thus, the routing decisions of the computers in the source site are simplified. By default, sites do not use site gates.

The following are the requirements for site gates.

- The computer must belong to a site to be a site gate for that site.
- The computer must be able to connect to each neighboring site.

Because sites configured with site gates are dependent on the site gate for all inter-site transmission of MSMQ messages, it is preferable to assign more than one site gate to a site, to provide load balancing and failure recovery.

site link

MSMQ measures inter-site routing based on costs assigned to links. You can assign link costs based on the delay of the link or the communications costs for the line (for example a dial-up line). If you have only two sites, choose any value above zero. If you have three or more sites, and the cost of routing between sites is more or less equal, use the same value for each site link. However, if you have three or more sites and the cost of routing between sites is not equal, use site-link costs to define the difference in the routing costs. A site-link cost of zero indicates that the two sites are not connected. Site link costs can range from 1 to 999,999.

If a site is configured to use a site gate, the site gate must belong to the same CN as a server in the other site. If the other site also uses a site gate, the site gate must belong to the same CN as the site gate in the other site.

site-link cost

MSMQ calculates the cost of inter-site routing based on relative numbers that administrators assign to site links. These numbers, called *site-link costs*, represent the cost of communication of that link. Site-link costs can be between 0 and 999,999. A site-link cost of zero indicates that two sites are not connected.

source journaling

The process of storing a copy of an outgoing message. Source journaling is configured on a message basis and is, therefore, a property set by the sending application. When source journaling is enabled for a message, a copy of the message is put in the source journal queue of the sending computer when the message arrives at the target queue. In MSMQ Explorer, the source journal queue is displayed under the computer.

source computer

The computer that sent the message.

supporting server

A PEC, PSC, BSC, or MSMQ routing server that supports one or more MSMQ dependent clients.

target journaling

The process of storing a copy of incoming messages. Target journaling is configured on a queue basis. When target journaling is enabled, a copy of each incoming message is placed in the target journal queue when the message is removed (read) from the target queue. A target journal queue (simply called Journal) is created for each queue when the queue is created. In MSMQ Explorer, target journal queues are displayed under each public queue.

transaction

A transaction is a unit of work that is carried out as an atomic operation—that is, the operation succeeds or fails as a whole. The unit of work is usually the pairing of two or more operations. The transaction ensures that the MSMQ message operations either succeed or fail in conjunction with other OLE-transaction-compliant operations or other MSMQ operations. For example, an MSMQ-based application can send a message and update an SQL Server database in the same transaction. MS DTC ensures that either both actions succeed or neither is executed.

MSMQ can be used as a resource manager under the control of Microsoft Distributed Transaction Coordinator (MS DTC) and is, therefore, compatible with any XA-compliant resource manager.

Using the MSMQ transaction flag you can.

- Transact the sending or receiving of any message with any other transactional resource (for example, updating an SQL database and sending a message) and transact the sending or receipt of multiple messages.
- Ensure that a message is delivered only once (also called exactly-once delivery).
- Ensure that all messages sent from one computer to another are delivered in order (also called in order delivery).
- Use positive or negative acknowledgments (ACKs and NACKs) to confirm messages reached or were successfully retrieved from the destination queue (also called end-to-end confirmation).

transaction dead letter queue

A transactional message that cannot reach the destination application is stored in the transaction dead letter queue on the source computer. Transaction dead letter queues are created for each independent client and server on your MSMQ network when MSMQ is installed on that computer. These queues are displayed as **Xact Dead Letter** under the computer in MSMQ Explorer.

type ID

See *queue type*.

XA-compliant

An XA-compliant resource manager uses the X/Open Distributed Transaction Processing XA interface to communicate with a transaction manager. XA-compliant transaction managers coordinate distributed transactions between XA-compliant resource managers. MS DTC is both an XA-compliant resource manager and an OLE transactions-compliant transaction manager. Because MSMQ is an OLE transactions-compliant resource manager, it can be XA-compliant through MS DTC.

To specify the cost of inter-site routing

1. Right-click a site, and then click **Properties**.
2. On the **Connections** tab, in **Links**, click the site, and then click **Edit**.
3. Specify a new cost, and then click **OK**.

Notes

- Inter-site routing is the process of routing messages between sites. MSMQ measures inter-site routing based on relative numbers that you assign to site links. Typically, you should define the relative cost of routing between sites using either cost or delay (the speed of one link versus another), although it is recommended that you use delay.
- If two wires connect a site, use the faster wire (lower cost).

To change the intra-site and inter-site database replication interval for a site

1 Right-click a site, and then click **Properties**.

2 On the **MQIS** tab, set the **External–Inter-Site** and **Internal–Intra-Site** replication intervals, and then click **OK**.

Notes

- These values affect only the selected site.
- To change the default intra-site and inter-site database replication intervals for all new sites, set the replication interval for the enterprise.

To change the default intra-site and inter-site database replication intervals

1 Right-click the enterprise, and then click **Properties**.

2 On the **MQIS Defaults** tab, set the **External–Inter-Site** and **Internal–Intra-Site** replication defaults.

Notes

- These values do not affect the inter-site or intra-site database replication for existing sites. They are used, by default, by all newly installed sites.
- To change the intra-site and inter-site database replication intervals for an individual site, set the replication interval for that site.

To define new site links

1 Right-click a site, and then click **Properties**.

2 On the **Connections** tab, in **Links**, click the site, and then click **Add**.

3 Specify the new site name and link cost, and then click **OK**.

Notes

- If a site is configured to use a site gate, the site gate must belong to the same CN as a server in the other site. If the other site also uses a site gate, the site gate must belong to the same CN as the site gate in the other site.
- MSMQ measures inter-site routing based on costs assigned to links. You can assign site-link costs based on the delay of the link or the communications costs for the line (such as a dial-up line). If you have only two sites, choose any value above zero. If you have three or more sites and the cost of routing between sites is approximately equal, use the same value for each site link. However, if you have three or more sites and the cost of routing between sites is not equal, use site-link costs to define the difference in the routing costs. A site-link cost of zero indicates that the two sites are not connected.
- Site link costs can range from 1 to 999,999.

To remove a site

1 Right-click a site, and then click **Delete**.

2 Click **Yes**.

Notes

- When you delete a site, all computer and queues within the site are deleted from the MQIS, and all site links to and from the deleted site are deleted.
- It is best to remove a site by uninstalling the site controller server (the PSC or PEC). When you uninstall a site, all links to neighboring sites are deleted from those sites.
- When you delete a site, all computers within the deleted site that have different original sites return to their respective original sites.
- To remove more than one site, click the **Sites** folder, click multiple sites in the right pane of MSMQ Explorer, right-click the selection, and then click **Delete**. To select a contiguous block of sites, hold down SHIFT while clicking the sites. To select non-adjacent sites, hold down CTRL while clicking the sites.

{button ,AL("A_REMOVE_QUEUE;A_REMOVE_COMPUTER;A_REMOVE_CN")} Related Topics

To remove a CN

1 In the **Connected Networks** folder, right-click a CN, and then click **Delete**.

2 Click **Yes**.

Notes

- When you attempt to delete a CN that is being used by an independent client and its assigned InRS or OutRS, MSMQ Explorer displays a warning message because the independent client will lose connectivity to the server if you delete the CN.
- To remove more than one CN, click the **Connected Networks** folder, click multiple CNs in the right pane of MSMQ Explorer, right-click the selection, and then click **Delete**. To select a contiguous block of CNs, hold down SHIFT while clicking the CNs. To select non-adjacent CNs, hold down CTRL while clicking the CNs.

{button ,AL("A_REMOVE_QUEUE;A_REMOVE_COMPUTER;A_REMOVE_SITE")} Related Topics

To remove a computer

1 Right-click a computer, and then click **Delete**.

2 Click **Yes**.

Notes

- When you remove a computer, all its queues are also removed.
- It is best to remove a computer by running Setup and clicking **Remove All**. When you uninstall a computer, it is automatically removed from the MQIS database.
- If the computer is an MSMQ server being used as an InRS or OutRS, it is removed from the InRS and OutRS lists of all independent clients using that server.
- If the computer is an MSMQ server being used as a site gate, the server is removed from the site's site-gate list.
- To remove more than one computer within the same site, click the site that contains the computers, click multiple computers in the right pane of MSMQ Explorer, right-click the selection, and then click **Delete**. To select a contiguous block of computers, hold down SHIFT while clicking the computers. To select non-adjacent computers, hold down CTRL while clicking the computers.

{button ,AL("A_REMOVE_QUEUE;A_REMOVE_CN;A_REMOVE_SITE")} Related Topics

To remove a queue

1 Right-click a queue, and then click **Delete**.

2 Click **Yes**.

Note

When you delete a queue all messages within the queue are also deleted.

{button ,AL("A_REMOVE_CN;A_REMOVE_SITE;A_REMOVE_COMPUTER")} Related Topics

To change a computer’s CN settings

1 Right-click a computer, and then click **Properties**.

2 Click the **Network** tab.

- To change a current CN setting, click either the IP or IPX in **Address List**, and then click **Edit**.
- To add a new CN assignment, click **Add**.
- To remove a CN assignment, click either the IP or IPX in **Address List**, and then click **Remove**.

Note

- Each computer must belong to at least one CN.

To create a new CN

1 Right-click the enterprise, point to **New**, and then click **CN**.

2 In **CN Name**, type the new CN name, and then select **IP**, **IPX**, or **Foreign**.

Note

A foreign CN contains foreign computers (a computer that does not run MSMQ or that belongs to another MSMQ enterprise) and an MSMQ connector server (a computer that handles messaging between your MSMQ enterprise and other message-queuing systems or MSMQ enterprises).

{button ,AL("A_CREATE_NEW_QUEUE;A_CREATE_FOREIGN_COMPUTER")} Related Topics

To create a new queue

1 Right-click a computer, point to **New**, and then click **Queue**.

2 In **Name**, type the new queue name.

3 Click **Transactional** to create a transactional queue.

{button ,AL("A_CREATE_NEW_CN")} Related Topics

To view computer performance data from MSMQ Explorer

- Right-click a computer, and then click **Properties**.
- To see status information, click the **Status** tab.
- To see MSMQ IS object data, click the **IS Status** tab.
- To run Performance Monitor, click **Performance Monitor**.

Notes

- The counters you see on the **Status** tab are a subset of counters available under the **MSMQ Queue** and **MSMQ Service** objects in Windows NT Performance Monitor.
- When viewing performance data from Windows NT Performance Monitor, you can view the data in chart, report, or alert views, or log the performance data to a file. For more information on Performance Monitor, see Windows NT Server version 4.0 *Concepts and Planning*.

{button ,AL("A_VIEW_QUEUE_PERF_DATA_EXP")} Related Topics

To view queue performance data from MSMQ Explorer

- Right-click a queue, and then click **Properties**.
- To see status information, click the **Status** tab.
- To run Performance Monitor, click **Performance Monitor**.

Notes

- The counters you see on the **Status** tab are a subset of counters available under the **MSMQ Queue** and **MSMQ Service** objects in Windows NT Performance Monitor.
- When viewing performance data from Windows NT Performance Monitor, you can view the data in chart, report, or alert views, or log the performance data to a file. For more information on Performance Monitor, see Windows NT Server version 4.0 *Concepts and Planning*.

{button ,AL("A_VIEW_COMPUTER_PERF_DATA_EXP")} Related Topics

To modify independent client InRS and OutRS settings

1. Right-click an independent client and then click **Properties**.
2. Click the **Routing** tab.
   - To add an InRS, under **In Routing Servers**, click **Add**.
   - To remove an InRS, under **In Routing Servers**, click the InRS, and then click **Remove**.
   - To change an InRS, under **In Routing Servers**, click the InRS, and then click **Edit**.
   - To add an OutRS, under **Out Routing Servers**, click **Add**.
   - To remove an OutRS, under **Out Routing Servers**, click the OutRS, and then click **Remove**.
   - To change an OutRS, under **Out Routing Servers**, click the OutRS, and then click **Edit**.
3. Click **OK** to save your changes.

Notes

- If an independent client is configured to use an InRS, every incoming message is first routed through the InRS and then routed to the independent client. If an independent client is configured to use an OutRS, every outgoing message is routed from the independent client to the OutRS. However, when an independent client is moved to another site, any InRS and OutRS settings are disabled until the independent client is returned to its original site.
- InRSs and OutRSs must be in the same site as the independent client and must have at least one CN in common with the independent client. The same MSMQ server can be used as an independent client's InRS and OutRS.
- Because independent clients configured with InRSs and OutRSs are dependent on the MSMQ server, it is preferable to assign more than one InRS or OutRS to independent clients to provide load balancing and failure recovery. You can assign up to three InRSs and three OutRSs.
- The PEC, PSCs, BSCs, and MSMQ routing servers can all be used as InRSs and OutRSs.

To modify site gate settings for a site

1. Right-click a site, and then click **Properties**.
2. Click the **Connections** tab.

- To add a site gate, under **Site Gates**, click **Add**.
- To edit a site gate, in **Site Gates**, click the computer name, and then click **Edit**.
- To remove a site gate, in **Site Gates**, click the computer name, and then, under **Site Gates**, click **Remove**.

3. Click **OK**.

Notes

- Inter-site session concentration is done by establishing site gates. If a site is configured to use a site gate, every MSMQ message sent between computers in different sites must be routed through the site gate. The routing topology beyond the source site is transparent to the computers within the site, with the exception of the site gate. This simplifies routing decisions. By default, sites do not use site gates.
- To be a site gate for the site, the computer must belong to the site. The computer must also be able to connect to each neighboring site.
- Because sites configured with site gates are dependent on the site gate for all inter-site transmission of MSMQ messages, it is preferable to assign more than one site gate to a site, to provide load balancing and failure recovery. There is no limit to the number of site gates

To enable message route tracking

1. Right-click the computer to track, and then click **Properties**.
2. On the **Tracking** tab, in **Pathname of Report Queue**, click the report queue.

   Or, to create a new report queue, click **New** and specify the full pathname (such as *mycomputer\myqueue*).
3. Click **Track only test message** or **Track all messages**.

Notes

- Implementing message route tracking is a two step process. First, the administrator must enable message route tracking by assigning a report queue. Second, the application must set the message property PROPID_M_TRACE to MQMSG_SEND_ROUTE_TO_REPORT_QUEUE. If the application developer does not set this property, message route tracking cannot occur. Test messages have PROPID_M_TRACE set to MQMSG_SEND_ROUTE_TO_REPORT_QUEUE.
- When you select **Track all messages**, all the messages sent from the computer report their routes to the report queue using report messages if the sending application has set the message route tracking flag. Tracking then occurs for messages that originate at the computer and messages routed by the computer (if it is an MSMQ routing server). When you select **Track only test messages**, report tracking messages are sent only for messages sent from the **Send Test Message** dialog box (available when you select a computer and then click **Send Test Messages** on the **Tools** menu).

To send a test message

1 Click a computer, click **Tools**, and then click **Send Test Message**.

The computer you select is the computer that will send the test message.

2 In **Destination Queue**, select the destination queue, specifying the full pathname (for example, *mycomputer*\ *myqueue*)**.**.

Or, click **New Queue**, and specify a new test queue and the full pathname.

3 Click **Send**.

Notes

- You can send test messages only to test queues. All test queues have a type ID of {55EE8F33-CCE9-11CF-B108-0020AFD61CE9}.
- If you change the type ID of a transactional queue to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9} and send test messages to the transactional queue, the messages are never delivered. Only transactional messages can be sent to transactional queues, and MSMQ Explorer test messages are not transactional. Similarly, if you change the type ID of a queue requiring authentication to {55EE8F33-CCE9-11CF-B108-0020AFD61CE9} and send test messages to the queue, the messages are not delivered (unless the target queue is located on the sending computer).
- Because all test messages are sent with message route tracking enabled, if the sending computer has a report queue, the message path of the test messages is tracked. For more information, see the *Microsoft Message Queue Server Administrator's Guide*, Chapter 4, "Monitoring Your MSMQ Enterprise."

To view events from MSMQ Explorer

1 In MSMQ Explorer, right-click any computer, and then click **Properties**.

2 Click the **Events** tab.

3 To view the events from Windows NT Event Viewer, click **Event Viewer**.

Note

When viewing events from Windows NT Event Viewer, you can sort, filter, and search for events, based on different event properties. For more information on Event Viewer, see Windows NT Server version 4.0 *Concepts and Planning*.

To rename the enterprise

1 Right-click the enterprise name , and then click **Rename**.

2 Type the new enterprise name, and click **OK**.

{button ,AL("A_RENAME_SITE;A_RENAME_CN")} Related Topics

To rename a site

1 In MSMQ Explorer, right-click any site, and then click **Rename**.

2 Type the new site name, and click **OK**.

{button ,AL("A_RENAME_ENTERPRISE;A_RENAME_CN")} Related Topics

To rename a CN

1 In the **Connected Networks** folder, right-click any CN, and then click **Rename**.

2 Type the new CN name, and click **OK**.

{button ,AL("A_RENAME_ENTERPRISE;A_RENAME_SITE")} Related Topics

To change a queue's type ID

1 Right-click a queue, and then click **Properties**.

2 In **Type ID**, type the new queue type ID.

Note

The queue type ID specifies the type of service provided by the queue. For example, if your application receives messages from a MAPI application, the application requires an input queue with a specific MAPI type-ID. The queue type ID can also be used to search for, open, or delete a specific type of queue.

{button ,AL("A_RENAME_QUEUE")} Related Topics

To change a queue label

1 Right-click a queue, and then click **Properties**.

2 In **Label**, type the new queue label.

{button ,AL("RENAME_QUEUE_TYPE_ID")} Related Topics

To set access control permissions

1 Right-click the enterprise, site, computer, or queue name, and then click **Properties**.

2 On the **Security** tab, click **Permissions**.

- To change permissions for everyone, click **Everyone**, and then click a **Type of Access**.
- To change permissions for the object owner, click the owner's account, and then click a **Type of Access**.
- To set permissions for a different user or group, click **Add**; then, in **Add Names**specify the user or group, and then click a **Type of Access**.
- To remove permissions for a user or group, in **Name**, select the user or group, and then click **Remove**.

3 Click **OK**.

{button ,AL("a_controlling_access;a_spec_perm")} Related Topics

To audit enterprise, site, computer, or queue access

1. Right-click the enterprise, site, computer, or queue name, and then click **Properties**.
2. On the **Security** tab, click **Auditing**.
3. Click **Add**.
4. Specify the users or groups to audit, and then click **OK**.
5. Click the events to audit, and then click **OK**.
6. If a message appears stating that the Audit Policy does not have auditing turned on, run User Manager and turn on auditing.

Notes

- You can track the usage of an enterprise, site, CN, computer, or queue with auditing. For a particular enterprise, site, CN, computer, or queue, you can specify which groups, users, and actions to audit. You can audit both successful and failed actions. The information generated by an audit is stored in the Windows NT security log.
- To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server), and then use MSMQ Explorer to specify which actions to audit for which objects and users, and whether or not to audit successful access, failed access, or both.

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_cn_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

To set security to allow multiple users to install MSMQ servers

1. Right-click the enterprise, and then click **Properties**.
2. On the **Security** tab, click **Permissions**.
3. Click **Add**, and then in **Add Names**, specify the user or group that you want to have permissions to install MSMQ servers.
4. In **Type of Access**, click **Full Control (All)**.

Note

In general, do not include local groups when setting permissions. Local groups are verifiable only on the computer on which they are defined. However, access rights are verified by many different MSMQ controller servers. To properly set up security, use the **Everyone** group and any global groups.

To find a computer

1 On the **Tools** menu, point to **Find**, and then click **Computer**.

2 Type the computer name, and (optionally) click the computer type.

You can search for **All Types**, **MSMQ routing servers**, **Backup site controllers**, and **Primary site controllers**.

3 Click **Find Now**.

Notes

- You can open multiple **Find** dialog boxes for computers and queues.
- When you search for a particular type of server, MSMQ Explorer returns of list of all servers that support the functionality of the server. For example, when you search for MSMQ routing servers, MSMQ Explorer returns a list of all MSMQ routing servers, BSCs, PSCs, and the PEC, because they all support MSMQ routing server functionality.

{button ,AL("A_FIND_QUEUE")} Related Topics

To find a queue

1 On the **Tools** menu, point to **Find**, and then click **Queue**.

2 Type the queue **Label** or **Type ID**.

3 Click **Find Now**.

Note

You can open multiple **Find** dialog boxes for computers and queues.

{button ,AL("A_FIND_COMPUTER")} Related Topics

To change the column display of MSMQ Explorer

1 On the **View** menu, click **Columns**.

2 On the **Message**, **Queue**, **Computer**, and **Site** tabs, under **Available Columns**, click the column you want to view.

3 In **Available Columns** or **Show the following**, click column names, and then click **Add** or **Remove**.

4 Click **OK** to save your changes.

{button ,AL("A_MQXPLORE_MESSAGE_COLUMNS;A_MQXPLORE_QUEUE_COLUMNS;A_MQXPLORE_COMPUTER_COLUMNS;A_MQXPLORE_SITE_COLUMNS")} Related Topics

To view private queues on a computer

- Right-click the computer, and then click **Show Private Queues**.

Notes

- A check mark appears next to **Show Private Queues** if it is already enabled.
- When you press F5 to refresh the display, private queues are no longer displayed.
- To view private queues for more than one computer within the same site, click the site that contains the computers, select multiple computers in the right pane of MSMQ Explorer, right-click the selection, and then click **Show Private Queues**. To select a contiguous block of computers, hold down SHIFT while clicking the computers. To select non-adjacent computers, hold down CTRL while clicking the computers.

To delete all messages in a queue

1 Right-click a queue, and then click **Purge**.

2 Click **Yes**.

To change a queue's priority

1 Right-click a queue, and then click **Properties**.

2 On the **Advanced** tab, specify the queue’s **Base Priority**.

Note

MSMQ routes and delivers messages based on a combination of queue priority, called the *base priority*, and message priority. Messages are routed and delivered by queue priority first, and message priority second. Queue priority for a public queue can be set at any time by any MSMQ-based application that has write permissions for the queue. The queue priority can be set from -32768 to 32767. The default priority setting is 0. Private queues do not support queue priority.

To specify whether a queue receives only authenticated messages

1 Right-click a queue, and then click **Properties**.

2 On the **Advanced** tab, click to clear or select the **Authenticated** check box.

Note

When you select the **Authenticated** check box, the queue accepts only authenticated messages unless the source computer is the same as the destination computer.

To enable or disable target journaling for a queue

1 Right-click a queue, and then click **Properties**.

2 On the **Advanced** tab, click to clear or select the **Enabled** check box.

Note

Target journaling is the process of storing a copy of all incoming messages. When target journaling is enabled, a copy of each incoming message is placed in the target journal queue when the message is removed (read) from the target queue. A target journal queue (simply called Journal) is created for each queue. MSMQ Explorer displays each queue’s target journal queue under the queue.

To limit the total size of messages that can be stored in a queue

1 Right-click a queue, and then click **Properties**.

2 On the **Advanced** tab, click **Limit message storage (in KB) to**, and then type the total size of all messages that can be stored in the queue.

Note

When the queue quota is reached, messages cannot be sent to the queue until the cumulative size of messages in the queue drops below the queue quota you specified.

{button ,AL("a_set_computer_quota;a_set_computer_journal_quota;a_specify_target_journal_quota")} Related Topics

To limit the total size of journal messages that can be stored on a computer

1 Right-click a queue, and then click **Properties**.

2 On the **Advanced** tab, click **Limit journal storage (in KB) to**, and type the total size of all messages that can be stored in the queue's journal queue.

Note

- Target journaling is the process of storing a copy of all incoming messages. When target journaling is enabled, a copy of each incoming message is placed in the target journal queue when the message is removed (read) from the target queue. The target journal queue (simply called Journal) is created each time a queue is created. MSMQ Explorer displays each queue's target journal queue under the queue.
- When the target journal queue quota is reached, target journaling stops.

{button ,AL("a_set_computer_quota;a_set_computer_journal_quota;a_specify_message_quota")} Related Topics

To specify whether a queue receives only encrypted messages

1. Right-click a queue, and then click **Properties**.
2. On the **Advanced** tab, click the queue's **Privacy Level**.
   - To have the queue accept private (encrypted) and non-private messages, click **Optional** (the default).
   - To have the queue accept only private messages, click **Body**.
   - To have the queue accept only unencrypted messages, click **None**.

Note

- The privacy level determines how the queue handles encrypted messages.
- If the destination queue is on the computer sending the message, unencrypted messages can be sent to a queue with a **Privacy Level** set to **Body**.

To determine if MSMQ independent clients and servers are online

- Right-click a computer, and click **MQPing**.

Notes

- When you ping a computer, MSMQ attempts to connect to the computer for 30 seconds, and updates the computer icon accordingly.
- When you press F5 to refresh the display, MQPing icons are no longer displayed.
- When a computer running MSMQ receives an MQPing request, it returns the contents of the request to a private queue called explorer_response_queue.
- To ping more than one computer within the same site, click the site that contains the computers, select multiple computers in the right pane of MSMQ Explorer, right-click the selection, and then click **Ping**. To select a contiguous block of computers, hold the SHIFT key while clicking the computers. To select non-adjacent computers, hold the CTRL key while clicking the computers.

To take ownership of an enterprise, site, CN, computer, or queue

1 Right-click an enterprise, site, CN, computer, or queue, and then click **Properties**.

2 On the **Security** tab, click **Ownership**.

3 Click **Take Ownership**.

Notes

- When you create an enterprise, site, CN, computer, or queue, you become the owner of it. By granting permissions, the owner controls how the enterprise, site, CN, computer, or queue is used. The owner can grant permission to another user to take ownership of the enterprise, site, CN, computer, or queue .
- When a local user (a user not logged on to a Windows NT domain) creates an object or takes ownership of the object, everyone has full control over the object.

{button ,AL("a_taking_ownership")} Related Topics

To create a foreign computer

1. Right-click the site in which you want to create the computer, point to **New**, and then click **Foreign Computer**.
2. In **Name**, type the foreign computer name.
3. Click the connected networks that the foreign computer will use, and then click **Add**.

Note

A foreign CN contains foreign computers (a computer that does not run MSMQ, or belongs to another MSMQ enterprise) and an MSMQ connector server (a computer that handles messaging between your MSMQ enterprise and other message queuing systems or other MSMQ enterprises).

{button ,AL("A_CREATE_NEW_CN")} Related Topics

To set the default time-to-reach-queue value for your enterprise

1 Right-click the enterprise, and then click **Properties**.

2 On the **General** tab, specify the **Default lifetime of a message in the network**.

Note

The default lifetime of a message in the network is 90 days.

To limit the number of messages that can be stored on a computer

1 Right-click a computer, and then click **Properties**.

2 On the **General** tab, click **Limit message storage (in KB) to**, and then type the total size of all messages that can be stored in all queues on the selected computer.

Note

When the computer quota is reached, messages cannot be sent to any queues on the computer until the cumulative size of messages in the queues drops below the queue quota.

{button ,AL("a_set_computer_journal_quota;a_specify_message_quota;a_specify_target_journal_quota")} Related Topics

To limit the number of journal messages that can be stored on a computer

1 Right-click a computer, and then click **Properties**.

2 On the **General** tab, click **Limit journal storage (in KB) to**, and then type the total size of all messages that can be stored in the selected computer's source journal queue.

Note

When the source journal queue quota is reached, source journaling ceases until the cumulative size of messages drops below the quota.

{button ,AL("a_set_computer_quota;a_specify_message_quota;a_specify_target_journal_quota")} Related Topics

To view the list of dependent clients for a particular server

1 Right-click a server, and then click **Properties**.

2 Click the **Dependent Clients** tab.

To enable auditing

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server), and then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether or not to audit successful access, failed access, or both.

Permissions

Use to set or change permissions for groups and users.
Click the following for information about this dialog box.

- Owner
- Name
- Type of Access
- Add
- Remove

{button ,AL("a_controlling_access;a_spec_perm;a_set_acl_perm")} Related Topics

Owner

Displays the name of the owner for the selected object (enterprise, site, CN, computer, or queue).

Name

Displays the names of groups and users and their current permissions.

Type of Access

Displays a list of available permissions.

Add

Adds selected groups and users to the permission list.

Remove

Removes selected groups and users from the permission list.

Special Access

Use to set special access permissions for the selected object (enterprise, site, CN, computer, or queue). These permissions can be set for a group or user.

Click the following for information about this dialog box:

- Name
- Full Control (All)
- Other

{button ,AL("a_controlling_access;a_spec_perm;a_set_acl_perm")} Related Topics

Name

Displays the name of the selected group or user.

Full Control (All)

When selected, grants all the special access permissions to the selected group or user.

Other

Displays the specific permissions you can set for a group or user.

Add Users and Groups

Use to add a group or user to the auditing or permissions list for an enterprise, site, CN, computer, or queue.

Click the following for information about this dialog box:

- List Names From
- Names
- Add
- Show Users
- Members
- Search
- Add Names
- Type of Access

{button ,AL("a_controlling_access;a_spec_perm;a_set_acl_perm")} Related Topics

Add Users and Groups

Used to add a group or user to the auditing or permissions list for an enterprise, site, CN, computer, or queue.

Click the following for information about this dialog box:

- List Names From
- Names
- Add
- Show Users
- Members
- Search
- Add Names

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_cn_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

List Names From

Displays the name of the domain or computer whose groups are shown in **Names**. An asterisk (*) following the domain or computer name indicates that local groups for that domain or computer are shown.

- To display groups and users in another domain or on the computer, click another domain or click the computer.

Names

Displays the groups (and users if **Show Users** is selected) that belong to the current domain or computer. You can add to the permissions list by selecting groups and users and then clicking **Add**.

- To add groups or users to the permissions list, select the group or user in **Names** and click **Add**.

Names

Displays the groups (and users if **Show Users** is selected) that belong to the current domain or computer. You can add to the permissions list by selecting groups and users and then clicking **Add**.

Add

Adds groups and users selected in **Names** to the permissions list.

Add

Adds groups and users selected in **Names** to the auditing list.

Show Users

Displays the names of users who belong to the domain or computer selected in **List Names From**. By default, only groups are displayed.

Members

Displays the members of the group selected in **Names**.

Search

Searches for the domain to which a selected user or group belongs. To add a group or user, you must know which domain contains the account.

Add Names

Displays the names of groups and users you are adding to the list. You can include other users and groups by selecting them in **Names** and then clicking **Add**. You can also include other users and groups by typing the names of groups and users in **Add Names**. Separate names with a semicolon.

If the group or user account is not located on the computer or domain shown in **List Names From**, in **Add Names**, type the computer or domain name followed by the group or user name. Separate the names with a backslash.

Type of Access

Displays a list of available permissions for a user or group.

Auditing

Use to audit the use of an enterprise, site, CN, computer, or queue by groups and users.

Click the following for information about this dialog box:

- Name
- Events to Audit
- Add
- Remove

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_cn_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

Name

Displays the names of currently audited groups and users.

Events to Audit

Used to set auditing events to record successes, failures, both, or neither for selected users or groups.

Add

Adds groups or users to the auditing list.

Remove

Removes selected groups or users from the auditing list.

Local Group Membership

Displays the members of the local group selected in the **Add Users and Groups** dialog box.

- To add the entire group membership to **Add Names** in the **Add Users and Groups** dialog box, click **Add**.

  Or, select only the members you want, and then click **Add**.

On a network running Windows NT Server, global groups that are members of a local group appear in the **Local Group Membership** list.

- To see the members of a global group, select the group in the Local Group Membership dialog box, and then click **Members**.

Global Group Membership

Displays the members of the global group selected in the **Add Users and Groups** dialog box or in the **Local Group Membership** dialog box.

- To include the group in **Add Names** in the **Add Users and Groups** dialog box, click **Add**.

  Or, select only the members you want, and then click **Add**.

Find Account

If you do not know the name of the domain that contains the user or group account, use the **Find Account** dialog box to locate the domain of an account on a Windows NT Server network.

Click the following for information about this dialog box

- Find User or Group
- Search All
- Search Only In
- Search
- Add

Find User or Group

Type the name of the group or user whose account you want to find.

Search All

Searches for the account in all the listed domains.

Search Only In

Limits the search for the account to the selected domains.

Search

Starts the search for the specified group or user.

Add

Adds the selected user or group in **Search Results** to **Add Names** in the **Add Users and Groups** dialog box.

Controlling Access

Using Windows NT Server security, you can control access to the enterprise, sites, CNs, computers, and queues. For information about controlling access to each object, click the following

- Enterprise Access Control
- Site Access Control
- CN Access Control
- Computer Access Control
- Queue Access Control

{button ,AL("a_spec_perm;a_set_acl_perm")} Related Topics

Controlling Enterprise Access

By default, everyone has Read permission for the enterprise, and the enterprise administrator (the person who installed the enterprise) has Full Control permission. With Read permission for an enterprise, users can retrieve the enterprise permissions settings and register certificates in the MQIS database. That is, users have Get Permissions and Create User permissions.

With Write permission for an enterprise, users can create sites, create CNs, retrieve the enterprise permissions settings, and register certificates in the MQIS database. That is, users have Create Site, Create CN, Get Permissions, and Create User permissions.

{button ,AL("a_spec_ent_perm")} Related Topics

Controlling Site Access

By default, everyone has Write permission for a site, and the site administrator (the person who installed the site) has Full Control permission. With Write permission for a site, users can retrieve the site's permissions settings and create a computer in the site. That is, users have Create Computer and Get Permissions permissions.

With Read permission for a site, users can retrieve the computer's permissions settings. That is, you have Get Permissions permissions.

You can specify Full Control, Read, Write, or Special Access permissions for all users and groups.

{button ,AL("a_spec_site_perm")} Related Topics

Controlling CN Access

By default, everyone has Read permission for a CN, and the CN administrator (the person who created the CN) has Full Control permission. With Read permission for a CN, users can retrieve the CN's permissions settings. That is, users have Get Permissions permissions.
Write permissions for a CN are identical to Read permissions.
You can specify Full Control, Read, Write, or Special Access permissions for all users and groups.

{button ,AL("a_spec_cn_perm")} Related Topics

Controlling Computer Access

By default, everyone has Write permission for a computer, and the computer administrator (the person who installed the computer) has Full Control permission. With Write permission for a computer, users can retrieve the computer's permissions settings and create queues on the computer. That is, users have Create Queue and Get Permissions permissions.

With Read permission for a computer, users can receive messages from the computer’s journal and dead-letter queues and retrieve the computer's permissions settings. That is, users have Receive Dead Let., Peek Dead Letter, Receive Journal, Peek Journal, and Get Permissions permissions.

You can specify Full Control, Read, Write, or Special Access permissions for all users and groups.

{button ,AL("a_spec_computer_perm")} Related Topics

Controlling Queue Access

By default, everyone has Send permission for a queue, and the queue administrator (the person who created the queue) has Full Control permission. With Send permission for a queue, users can retrieve the queue's properties and permissions settings and send messages to the queue. That is, users have Send Message, Get Properties, and Get Permissions permissions.

With Receive permission for a queue, users can retrieve the queue's properties and permissions settings and view or receive messages from the queue. That is, users have Receive Journal, Receive Message, Peek Message, Get Properties, and Get Permissions permissions.

You can specify Full Control, Receive, Send, or Special Access permissions for all users and groups.

{button ,AL("a_spec_queue_perm")} Related Topics

Special Access Permissions

You can set special access permissions for the enterprise, sites, CNs, computers, and queues. For information about setting special access permissions, click the following

- Enterprise
- Site
- CN
- Computer
- Queue

{button ,AL("a_spec_access_perm;a_set_acl_perm")} Related Topics

Enterprise Special-Access Permissions

You can set the following enterprise special-access permissions for a selected user or group.

Create Site (Cs)
Used to create a site

Create CN (Cc)
Used to create a connected network

Create User (Cu)
Used to register certificates in the MQIS

Set Properties (Sp)
Used to set enterprise properties

Delete Enterprise (D)
Used to delete the enterprise

Get Permissions (Pg)
Used to view the enterprise permissions

Set Permissions (Ps)
Used to set the enterprise permissions

Take Ownership (O)
Used to take ownership of the enterprise

Note

- If you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.

{button ,AL("a_spec_site_perm;a_spec_cn_perm;a_spec_computer_perm;a_spec_queue_perm")} Related Topics

Site Special-Access Permissions

You can set the following site special-access permissions for a selected user or group.

Create Route server (Cr)
Used to install an MSMQ routing server in the site

Create BSC (Cb)
Used to install a BSC in the site

Create Computer (C)
Used to create a computer

Set Properties (Sp)
Used to set site properties

Delete Site (D)
Used to delete the site

Get Permissions (Pg)
Used to view site permissions

Set Permissions (Ps)
Used to set site permissions

Take Ownership (O)
Used to take ownership of the site

Note

- If you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.

{button ,AL("a_spec_ent_perm;a_spec_cn_perm;a_spec_computer_perm;a_spec_queue_perm")} Related Topics

CN Special-Access Permissions

You can set the following CN special-access permissions for a selected user or group.

Open Connector
Used to run an MSMQ connector application or service on the server

Set Properties (Sp)
Used to set CN properties

Delete CN (D)
Used to delete the CN

Get Permissions (Pg)
Used to view CN permissions

Set Permissions (Ps)
Used to set CN permissions

Take Ownership (O)
Used to take ownership of the CN

Note

- If you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.

{button ,AL("a_spec_ent_perm;a_spec_site_perm;a_spec_computer_perm;a_spec_queue_perm")} Related Topics

Computer Special-Access Permissions

You can set the following computer special-access permissions for a selected user or group.

Receive Dead Let. (Rd)
Used to receive dead-letter messages from the computer's dead-letter queue

Peek Dead Letter (Pd)
Used to view all dead-letter messages on the computer's dead-letter queue

Receive Journal (Rj)
Used to receive journal messages from the computer's journal queue

Peek Journal (Pj)
Used to view all journal messages on the computer's journal queue

Create Queue (C)
Used to create queues on the computer

Set Properties (Sp)
Used to set the computer properties

Delete Computer (D)
Used to delete the computer

Get Permissions (Pg)
Used to view computer permissions settings

Set Permissions (Ps)
Used to change permissions for a computer

Take Ownership (O)
Used to take ownership of the computer

Notes

- If you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.
- When you use MSMQ Explorer to grant either Receive Dead Let. or Receive Journal permissions to a user or group, that user or group also automatically gets the Peek Dead Letter and Peek Journal permissions (respectively). You can assign the Receive Dead Let. and Receive Journal permissions without assigning the Peek Dead Letter and Peek Journal permissions only programmatically; you cannot do so using MSMQ Explorer.

{button ,AL("a_spec_ent_perm;a_spec_site_perm;a_spec_cn_perm;a_spec_queue_perm")}
Related Topics

Queue Special-Access Permissions

You can set the following queue special-access permissions for a selected user or group.

Receive Journal (Rj)
Used to read journal messages from the queue

Receive Message (Rq)
Used to read messages from the queue

Peek Message (Pq)
Used to view messages in the queue and queue journal

Send Message (Sq)
Used to send a message to the queue

Set Properties (Sp)
Used to set the queue properties

Get Properties (Gp)
Used to view the queue properties

Delete Queue (D)
Used to delete the queue

Get Permissions (Pg)
Used to view the queue permissions settings

Set Permissions (Ps)
Used to change permissions for the queue

Take Ownership (O)
Used to take ownership of the queue

Notes

- If you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.
- When you use MSMQ Explorer to grant either Receive Message or Receive Journal permissions to a user or group, that user or group also automatically gets the Peek Message permission. You can assign the Receive Message permission without assigning the Peek Message permission only programmatically; you cannot do so using MSMQ Explorer.

{button ,AL("a_spec_ent_perm;a_spec_site_perm;a_spec_cn_perm;a_spec_computer_perm")}
Related Topics

Auditing Enterprise Events

Use auditing to record which users access which objects, the type of access attempted, and whether that access succeeded or failed. Audited events are recorded in the Windows NT security log and can be viewed from Windows NT Event Viewer.

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server); then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether to audit successful access, failed access, or both.

You can audit the following successful or failed enterprise actions for individual users or groups.

Create Site (Cs)
Audits the installation of a site

Create CN (Cc)
Audits the creation of CNs

Create User (Cu)
Audits the registration of certificates in the MQIS

Set Properties (Sp)
Audits changes to the enterprise properties

Delete Enterprise (D)
Audits the deletion of the enterprise

Get Permissions (Pg)
Audits the display of enterprise permissions

Set Permissions (Ps)
Audits changes to the enterprise permissions

Take Ownership (O)
Audits changes to enterprise ownership

Note

- To write messages to the security audit log, the user account that runs the MSMQ service must have the Generate security audits right. If the account does not have this right, the MSMQ service writes a warning message in the application log. By default, the MSMQ service runs in the local system account. By default, this account has the required right.

{button ,AL("a_set_audit_proc;a_audit_site_events;a_audit_cn_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

Auditing Site Events

Use auditing to record which users access which objects, the type of access attempted, and whether that access succeeded or failed. Audited events are recorded in the Windows NT security log and can be viewed from Windows NT Event Viewer.

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server); then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether to audit successful access, failed access, or both.

You can audit the following successful or failed site actions for individual users or groups.

Create Route Server (Cr)
Audits the installation of an MSMQ routing server

Create BSC (Cb)
Audits the installation of a backup site controller

Create Computer (C)
Audits the installation of an MSMQ independent client or server

Set Properties (Sp)
Audits changes to the site properties

Delete Site (D)
Audits the deletion of a site

Get Permissions (Pg)
Audits the display of site permissions

Set Permissions (Ps)
Audits changes to the site permissions

Take Ownership (O)
Audits changes to site ownership

Note

- To write messages to the security audit log, the user account that runs the MSMQ service must have the Generate security audits right. If the account does not have this right, the MSMQ service writes a warning message in the application log. By default, the MSMQ service runs in the local system account. By default, this account has the required right.

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_cn_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

Auditing CN Events

Use auditing to record which users access which objects, the type of access attempted, and whether that access succeeded or failed. Audited events are recorded in the Windows NT security log and can be viewed from Windows NT Event Viewer.

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server); then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether to audit successful access, failed access, or both.

You can audit the following successful or failed CN actions for individual users or groups.

Open Connector
Audits the running of an MSMQ connector application.

Set Properties (Sp)
Audits changes to CN properties

Delete CN (D)
Audits the deletion of a CN

Get Permissions (Pg)
Audits the display of CN permissions

Set Permissions (Ps)
Audits changes to CN permissions

Take Ownership (O)
Audits changes to CN ownership

Note

- To write messages to the security audit log, the user account that runs the MSMQ service must have the Generate security audits right. If the account does not have this right, the MSMQ service writes a warning message in the application log. By default, the MSMQ service runs in the local system account. By default, this account has the required right.

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_computer_events;a_audit_queue_events")} Related Topics

Auditing Computer Events

Use auditing to record which users access which objects, the type of access attempted, and whether that access succeeded or failed. Audited events are recorded in the Windows NT security log and can be viewed from Windows NT Event Viewer.

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server); then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether to audit successful access, failed access, or both.

You can audit the following successful or failed computer actions for individual users or groups.

Receive Dead Let. (Rd)
Audits the receipt of undeliverable (dead-letter) messages

Receive Journal (Rj)
Audits the receipt of journal messages

Create Queue (C)
Audits the creation of a queue

Set Properties (Sp)
Audits changes to the queue properties

Delete Computer (D)
Audits the deletion of a computer

Get Permissions (Pg)
Audits the display of queue permissions

Set Permissions (Ps)
Audits changes to the queue permissions

Take Ownership (O)
Audits changes to computer ownership

Note

- To write messages to the security audit log, the user account that runs the MSMQ service must have the Generate security audits right. If the account does not have this right, the MSMQ service writes a warning message in the application log. By default, the MSMQ service runs in the local system account. By default, this account has the required right.

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_cn_events;a_audit_queue_events")} Related Topics

Auditing Queue Events

Use auditing to record which users access which objects, the type of access attempted, and whether that access succeeded or failed. Audited events are recorded in the Windows NT security log and can be viewed from Windows NT Event Viewer.

To enable auditing, you must set the audit policy for all MSMQ servers (using User Manager for Domains on each server); then use MSMQ Explorer to specify which actions to audit, for which objects, for which users, and whether to audit successful access, failed access, or both.

You can audit the following successful or failed queue actions for individual users or groups.

Receive Journal (Rj)
Audits the reading of a journal message

Receive Message (Rq)
Audits the reading of a message

Set Properties (Sp)
Audits changes to the enterprise properties

Get Properties (Gp)
Audits the display of enterprise properties

Delete Queue (D)
Audits the deletion of a queue

Get Permissions (Pg)
Audits the display of enterprise permissions

Set Permissions (Ps)
Audits changes to the enterprise permissions

Take Ownership (O)
Audits changes to queue ownership

Note

- To write messages to the security audit log, the user account that runs the MSMQ service must have the Generate security audits right. If the account does not have this right, the MSMQ service writes a warning message in the application log. By default, the MSMQ service runs in the local system account. By default, this account has the required right.

{button ,AL("a_set_audit_proc;a_audit_ent_events;a_audit_site_events;a_audit_cn_events;a_audit_computer_events")} Related Topics

Owner

Displays the owner of the selected object (enterprise, site, CN, computer, or queue).

- To take ownership of the selected object, click **Take Ownership**.

Note

- When you take ownership on an object, you control how permissions are set on the object. You must have the Take Ownership permission for an object to take ownership of that object. By default, only those users that have Full Control permissions for an object have the Take Ownership permission. However, if you have the Take Ownership permission on a PEC, PSC, or BSC, you can take ownership of any object within the enterprise without explicitly having the Take Ownership permission on the specific object.

Enterprise Access Permissions

You can set the following standard permissions on the enterprise.

- Full Control (All)
- Read
- Write

By default, everyone has Read permissions for the enterprise, and the enterprise administrator (the person who installed the enterprise) has Full Control (All) permissions.

{button ,AL("a_site_access_perm;a_cn_access_perm;a_computer_access_perm;a_queue_access_perm")} Related Topics

Full Control (All) Permission for an Enterprise

The selected user or group can use this permission to

- Create a site
- Create a connected network
- Register certificates in the MQIS database
- Set enterprise properties
- Delete the enterprise
- View enterprise permissions
- Set enterprise permissions
- Take ownership of the enterprise

Read Permission for an Enterprise

The selected user or group can use this permission to

- ☐ View enterprise permissions

Write Permission for an Enterprise

The selected user or group can use this permission to

- Create a site
- Create a connected network
- Set enterprise properties
- Set enterprise permissions

Site Access Permissions

You can set the following standard permissions on a site.

- Full Control (All)
- Read
- Write

By default, everyone has Write permission for a site, and the site administrator (the person who installed the site) has Full Control (All) permission.

{button ,AL("a_ent_access_perm;a_cn_access_perm;a_computer_access_perm;a_queue_access_perm")} Related Topics

Full Control (All) Permission for a Site

The selected user or group can use this permission to

- Install an MSMQ routing server in the site
- Install a BSC in the site
- Create a computer
- Set site properties
- Delete the site
- View site permissions
- Set site permissions
- Take ownership of the site

Read Permission for a Site

The selected user or group can use this permission to

- ☐ View site permissions

Write Permission for a Site

The selected user or group can use this permission to

- Create a computer
- View site permissions

CN Access Permissions

You can set the following standard permissions on a CN.

- Full Control (All)
- Read
- Write

By default, everyone has Read permission for a CN, and the CN administrator (the person who installed the CN) has Full Control (All) permission.

Note

- For CNs, Read and Write permissions are the same.

{button ,AL("a_ent_access_perm;a_site_access_perm;a_computer_access_perm;a_queue_access_perm")} Related Topics

Full Control (All) Permission for a CN

The selected user or group can use this permission to

- Run an MSMQ connector application or service on the server
- Set CN properties
- Delete the CN
- View CN permissions
- Set CN permissions
- Take ownership of the CN

Read Permission for a CN

The selected user or group can use this permission to

- Set CN permissions

Write Permission for a CN

The selected user or group can use this permission to

- ☐ Set CN permissions

Computer Access Permissions

You can set the following standard permissions on a computer.

- Full Control (All)
- Read
- Write

By default, everyone has Write permission for a computer, and the person who installed the computer has Full Control (All) permission.

{button ,AL("a_ent_access_perm;a_site_access_perm;a_cn_access_perm;a_queue_access_perm")} Related Topics

Full Control (All) Permission for a Computer

The selected user or group can use this permission to

- Receive dead-letter messages from the computer's dead-letter queue
- View all dead-letter messages on the computer's dead-letter queue
- Receive journal messages from the computer's journal queue
- View all journal messages on the computer's journal queue
- Create queues on the computer
- Set computer properties
- Delete the computer
- View computer permissions settings
- Change permissions for a computer
- Take ownership of the computer

Read Permission for a Computer

The selected user or group can use this permission to

- Receive dead-letter messages from the computer's dead-letter queue
- View all dead-letter messages on the computer's dead-letter queue
- Receive journal messages from the computer's journal queue
- View all journal messages on the computer's journal queue
- View computer permissions settings

Write Permission for a Computer

The selected user or group can use this permission to

- Create queues on the computer
- View computer permissions settings

Queue Access Permissions

You can set the following standard permissions on a queue.

- Full Control (All)
- Receive
- Send

By default, everyone has Send permission for a queue, and the person who created the queue has Full Control (All) permission.

{button ,AL("a_ent_access_perm;a_site_access_perm;a_cn_access_perm;a_computer_access_perm")} Related Topics

Full Control (All) Permission for a Queue

The selected user or group can use this permission to

- Read journal messages from the queue
- Read messages from the queue
- View messages in the queue and queue journal
- Send a message to the queue
- Set queue properties
- View queue properties
- Delete the queue
- View queue permissions settings
- Change permissions for the queue
- Take ownership of the queue

Receive Permission for a Queue

The selected user or group can use this permission to

- Read journal messages from the queue
- Read messages from the queue
- View messages in the queue and queue journal
- View queue properties
- View queue permissions settings

Send Permission for a Queue

The selected user or group can use this permission to

- Send a message to the queue
- View queue properties
- View queue permissions settings

Remove user certificates

Use to select a user account when you need to delete some or all of its certificates.

- **List Names From** displays the name of the domain or computer whose groups are shown in **Names**. An asterisk (*) following the domain or computer name indicates that local groups for that domain or computer are shown. To display groups and users in another domain or on the computer, click another domain or click the computer.
- **Names** displays the users that belong to the currently selected domain or computer. To remove the user certificate for a user, click that user in **Names**, and then click **Add**.
- **Members** is not available in this dialog box.
- Click **Search** to search for the domain to which a user belongs. To remove a certificate for a user, you must know which domain contains the account.
- **Add Name** displays the name of the user whose user certificate you intend to remove.

Find Account

If you do not know the name of the domain that contains the user or group account, use the **Find Account** dialog box to locate the domain of an account on a Windows NT Server network.

Click the following for information about this dialog box

- Find User or Group
- Search All
- Search Only In
- Search
- Add

Find Account

If you do not know the name of the domain that contains the user or group account, use the **Find Account** dialog box to locate the domain of an account on a Windows NT Server network.

Click the following for information about this dialog box

- Find User or Group
- Search All
- Search Only In
- Search
- Add

MSMQ Explorer Overview

MSMQ Explorer displays a logical view of your MSMQ enterprise network. Using MSMQ Explorer, you can view and modify the properties of the following:

- Enterprise
- Sites
- Connected Networks
- Computers
- Queues

MSMQ Explorer displays only those computers that run the MSMQ service (independent clients, MSMQ routing servers, BSCs, PSCs, and the PEC). MSMQ dependent clients are not displayed. However, MSMQ connector servers (supporting foreign CNs, foreign computers, and foreign queues) are displayed. MSMQ Explorer uses a variety of icons to represent the different types of computers, queues, and messages.

Click here  to see a table of the MSMQ Explorer icons.

Information displayed in MSMQ Explorer may not be current because of MQIS replication delays. Changes you make from within MSMQ Explorer may not be displayed until replication takes place. For example, when you add a queue to a computer in site C from a computer in site B, you do not see the change in MSMQ Explorer until the MQIS change replicates from site C to site B, regardless of which site contains the PEC. The MSMQ Explorer display is not updated automatically. To update the display, press F5.

MSMQ Explorer Icons

The following table shows the MSMQ Explorer icons.


The MSMQ Enterprise


A site


A connected network


A PEC


A PSC


A BSC


An MSMQ routing server


An MSMQ independent client


Indicates the computer is online


Indicates the computer is offline


A public queue


A private queue


A journal queue


A dead-letter queue or transaction dead-letter queue


A message


A journal message


A report message


An acknowledgement message


A negative acknowledgement message


A test message


A dead letter

Note

The MQPing-related icons shown in the preceding table display on top of the computer icon. For example, an independent client that is online displays as follows:  .

MSMQ Explorer Message Columns

MSMQ Explorer displays a variety of information in the right pane when you click a public queue, computer, site, or the site folder. The following message columns are displayed when you click a public queue.

- Admin Queue
- Admin queue name len
- Arrived
- Authenticated
- Body
- Class
- Correlation
- Delivery Mode
- Destination Queue
- Destination queue name len
- Encrypted
- Encryption Algorithm
- Hash Algorithm
- Label
- Label Length
- Message ID
- Position In Queue
- Priority
- Response Queue
- Response queue name len
- Sender ID
- Sender ID Exist
- Sender ID Length
- Sent
- Size
- Source Computer
- Tracked

Label, Priority, Message ID, Position In Queue, and Size are displayed by default.

{button ,AL("A_MQXPLORE_QUEUE_COLUMNS;A_MQXPLORE_COMPUTER_COLUMNS;A_MQXPLORE_SITE_COLUMNS")} Related Topics

Displays the correlation ID set by the sending application. The correlation ID is used to correlate between a response message and the original message.

Displays **Express** or **Recoverable**, indicating the message delivery method.

Displays the length, in bytes, of the message label.

Displays the format name of the queue where administrative (acknowledgement) messages are sent.

Displays the length, in bytes, of the administrative queue format name.

Displays the date and time the message arrived at the destination queue.

Displays the body of the message. If the message body contains text data, this information is readable. If the message body contains binary information, this dialog box displays hexadecimal data along with its text translation.

If the body of the message contains Unicode characters, the message text is readable when displaying the message body in column view. However, the message body is not readable when you view the Body properties for the message. When you view the message properties, Unicode characters are displayed as 2-byte values.

Displays the format name of the message’s original destination queue. This column is most useful when viewing messages in journal and dead-letter queues (because the current queue is not the same as the original destination queue).

Displays the length, in bytes, of the destination queue’s format name.

Displays **Yes** or **No**, indicating whether the message is encrypted.

Displays the format name of the queue where response messages are sent.

Displays the length, in bytes, of the response queue’s format name

Displays the SID of the user who was logged on to the source computer when the message was sent.

The sending application can either provide the Sender ID property, or can request that the SID not be attached to the message (thereby creating an anonymous message). If the sender ID is not available, nothing is displayed.

When you display the message properties, the full user name is displayed in the domain\user ID format.

Displays **Yes** or **No**, indicating whether the sender of this message was identified.

The sending application can either provide the Sender ID property, or can request that the SID not be attached to the message (thereby creating an anonymous message).

Specifies the length, in bytes, of the SID of the user who is logged on to the source computer.

Displays the date and time the message was sent from the source computer.

Displays the GUID of the computer that sent the message.

Displays **Yes** or **No**, indicating whether message route tracking was enabled for the message.

Displays the numerical position of all messages in the selected queue. The position of messages within the queue is determined first by priority and then by message ID.

Displays the priority of each message in the queue.

Displays the size, in bytes, of each message in the queue.

Displays the GUID of each message in the queue.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer created by an algorithm. The algorithm uses several criteria to ensure that it is unique, including the current date, time, and a computer identifier. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the label of each message in the queue. The sending application specifies the message label.

Indicates whether each message in the queue is authenticated.

Indicates the message type. A message can be a normal MSMQ message, a positive or negative acknowledgment message, or a report message. All messages created by MSMQ-based applications are normal MSMQ messages.

Indicates which encryption algorithm the sending application used to encrypt the message body. The two possible encryption values are RC2 and RC4. If the message is not encrypted, nothing is displayed.

For more information on the various encryption algorithms that can be used with MSMQ, see the Microsoft CryptoAPI documentation.

Displays the hashing algorithm used for the message digest. The hashing algorithm values are defined by the sending application.

MSMQ Explorer Queue Columns

MSMQ Explorer displays a variety of information in the right pane when you click a public queue, computer, site, or the site folder. The following queue columns are displayed when you click a computer.

- Authenticated
- Base Priority
- Created
- ID
- Journal
- Journal Quota
- Label
- Modified
- Pathname
- Privacy Level
- Quota
- Transaction
- Type

Pathname, Label, Journal, Created, and Modified are displayed by default.

{button ,AL(`A_MQXPLORE_MESSAGE_COLUMNS;A_MQXPLORE_COMPUTER_COLUMNS;A_MQXPLORE_SITE_COLUMNS')} Related Topics

Displays the pathname of each queue in the selected computer.

Displays the label of each queue in the selected computer.

Indicates whether target journaling is enabled for each queue displayed.

Target journaling is the process of storing a copy of all incoming messages. When target journaling is enabled, a copy of each incoming message is placed in a *target-journal queue* when the message is removed (read) from the target queue. A target-journal queue (called **Journal**) is created for each queue when the queue is created. In MSMQ Explorer, a target-journal queue is displayed under each queue.

Displays the date that each queue in the selected computer was created.

Displays the date that each queue in the selected computer was modified.

Indicates whether each queue in the selected computer accepts only authenticated messages.

Displays the base priority of each queue in the selected computer. The base priority can be set from -32768 to 32767. The default is zero.

Displays the GUID of each queue in the selected computer.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer created by an algorithm. The algorithm uses several criteria to ensure that it is unique, including the current date, time, and a computer identifier. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the journal quota for each queue in the selected computer.

The journal quota specifies, in kilobytes, the total size of all messages that can reside in the queue at any time. When the target-journal queue quota is reached, target journaling ceases until the combined size of the messages in the queue drops below the journal quota.

Displays the privacy level required by each queue in the selected computer.

If the privacy level is None, the queue accepts only unencrypted messages. If the privacy level is Optional (the default), the queue accepts both unencrypted and encrypted messages. If the privacy level is Body, the queue accepts only encrypted messages.

If the destination queue is on the computer sending the message, unencrypted messages can be sent with the Privacy Level set to Body.

Indicates the quota (in kilobytes) for each queue in the selected computer. When the queue quota is reached, messages can no longer be sent to the queue.

Indicates whether each queue in the selected computer accepts only transactional messages.

Displays the queue’s type ID.

The queue’s type ID specifies the type of service provided by the queue. For example, if your application receives messages from a MAPI application, your application requires an input queue with a specific MAPI type-ID. You can also use the queue type-ID to look for, open, or delete a specific type of queue.

MSMQ Explorer Computer Columns

MSMQ Explorer displays a variety of information in the right pane when you click a public queue, computer, site, or the site folder. The following computer columns are displayed when you click a site.

- Computer Pathname
- Created
- Foreign Computer
- ID
- Journal Quota
- Modified
- Quota
- Service
- Type

Computer Pathname, Service, Created, Modified, and Foreign Computer are displayed by default.

{button ,AL(`A_MQXPLORE_MESSAGE_COLUMNS;A_MQXPLORE_QUEUE_COLUMNS;A_MQXPLORE_SITE_COLUMNS') } Related Topics

Displays the source-journal queue quota for each computer in the site. The journal quota specifies, in kilobytes, the total size of all messages that can reside in the source-journal queue. When the source-journal queue quota is reached, source journaling ceases until the cumulative size of messages drops below the quota.

Displays the computer quota for each computer in the site. When the computer quota is reached, messages cannot be sent to any queues on the computer until the cumulative size of messages in the queues drops below the queue quota.

Displays each computer’s operating system name, operating system version, and the version of MSMQ installed.

Displays the computer name for the computers in a selected site.

Displays the GUIDs for the computers in a selected site.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer created by an algorithm. The algorithm uses several criteria, including the current date, time, and a computer identifier, to ensure that it is unique. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the functions of the computers in a selected site. Computers can be independent clients, MSMQ routing servers, BSCs, PSCs, or PECs.

Because MSMQ dependent clients do not run the MSMQ service, they do not appear in MSMQ Explorer.

Displays the dates the computers in a selected site were created.

Displays the dates the computers in a selected site were last modified.

Displays **Yes** or **No**, indicating whether the computer is a connector server. **Yes** indicates that the computer is a connector server. **No** indicates that the computer is not a connector server but the computer is running MSMQ.

MSMQ supports the Windows NT and Windows 95 platforms. Level 8 Systems provides a product that supports the MSMQ API on many platforms including IBM MVS and CICS; Sun Solaris, HP-UNIX, and AIX UNIX platforms; as well as OS/2, VMS, and AS/400 platforms. The Level 8 Systems product also supports the mapping of native IBM MQSeries API (MQI) calls to the MSMQ API to provide seamless message exchange between IBM MQSeries applications and MSMQ-based applications. Any server running the Level 8 product is referred to as a connector server.

MSMQ Explorer Site Columns

MSMQ Explorer displays a variety of information in the right pane when you click a public queue, computer, site, or the site folder. The following site columns are displayed when you click the **Sites** folder.

- ID
- Server
- Site Pathname

All three column are displayed by default.

{button ,AL(`A_MQXPLORE_MESSAGE_COLUMNS;A_MQXPLORE_QUEUE_COLUMNS;A_MQXPLORE_COMPUTER_COLUMNS')} Related Topics

Displays the GUIDs for all sites in an enterprise.

A globally unique identifier (GUID) is a 128-bit (16-byte) integer created by an algorithm. The algorithm uses several criteria to ensure that it is unique, including the current date, time, and a computer identifier. The GUID format is {12345678-1234-1234-1234-123456789012}.

Displays the computer name for all site servers.

Displays the path for all sites in the enterprise.