



SMTP Site


There is one SMTP site for Microsoft SMTP Service. You cannot create additional sites or delete the existing one. Use the **SMTP Site** property sheet to name the site, identify the IP address, and set the connection type and limits. By default, the SMTP site can respond to connection requests for all IP addresses configured on the computer.

-  Description
-  IP Address
-  TCP Port
-  Limited To
-  Connection Time-out (Seconds)
-  Limit Connections per Domain
-  Enable Logging
-  Active Log Format

Advanced SMTP Site Identification

You can add IP addresses for the site and designate ports for each address. You cannot use the same port for more than one IP address.

 IP Address

 TCP Port

TCP Port

Type the port to be used for SMTP. The default is port 25. You cannot use the same port for more than one IP address.

IP Address

Select an IP address.

Advanced Multiple SMTP Site Configuration

If you have multiple IP addresses configured for the SMTP site, you can identify the TCP port for each address.

Active Log Format

You can choose one of four logging formats to track message transactions. The Microsoft Internet Information Server (IIS) Log File Format is a fixed ASCII format. The W3C Extended Log File Format is an ASCII format that can be customized and is the default option. You can choose the items you want to track. The National Center for Supercomputing Applications (NCSA) Common Log File Format is a fixed ASCII format. The ODBC logging format uses an ODBC-compliant database to store logged data for a fixed set of data fields.

Description

Type the name of the SMTP site. You can change the default name, but you cannot delete the site.

IP Address

The SMTP site can respond to connection requests for all IP addresses configured on the computer.

TCP port

Type the TCP port to be used for incoming and outgoing transmissions. The default is port 25 for both types of connections.

Limited to

For incoming connections, this setting specifies the number of concurrent connections. The default is 1000. The minimum value is 1 connection.

For outgoing connections, this setting specifies the total number of outbound connections to all remote domains that can exist at one time. The default is 500. The minimum value is 1 connection.

Connection Time-out (Seconds)

If a connection is inactive for a designated period of time, Microsoft SMTP Service closes it. You can specify this time period. The default is 600 seconds for both incoming and outgoing connections.

Limit Connections per Domain

This setting limits the number of outgoing connections to any single remote domain. The default is 100. The value should be less than or equal to the value for the **Limited to** option under **Outgoing Connections**.

Maximum Number of Outbound Messages per Connection

This option enables you to limit the number of messages sent in a single connection. It also provides a method to increase system performance by using multiple connections to deliver messages to a remote domain. Consequently, once the set limit is reached, a new connection is automatically opened and the transmission continues until all messages are delivered.

For example, if you commonly send a large number of messages to certain remote domains, then you could set the **Maximum number of outbound messages per connection** value to a relatively small number such as 20. As a result, when sending 100 messages in one session, Microsoft SMTP Service immediately opens a new connection after the first 20 are sent, then another connection after the next 20 are sent, and so on. In this case, there could be up to five simultaneous connections delivering queued mail to one destination. Message delivery would be faster, because smaller numbers of messages are delivered simultaneously instead of in one long stream over one connection.

To determine a value for the limit, review the **Messages Sent/sec** performance counter for the **SMTP Server** object in Performance Monitor. The **Maximum number of outbound messages per connection** value should be less than the value indicated by the performance counter. If the counter indicates a value of 30, and you set your maximum connections to 50, no simultaneous connection would be opened because the server wouldn't exceed 30 messages per second. It would work as though the messages were sent in one long stream over one connection. This setting affects only outgoing messages and you can use it to increase your server output speed. The rate that receiving servers process incoming messages varies.

Perform Reverse DNS Lookup on Incoming Messages

If you select this option, Microsoft SMTP Service can verify that the IP address for the domain in the *From* line matches the originating IP address noted in the header. This address confirms that the message originated from the computer and domain listed in the *From* field. If the reverse DNS lookup is successful, the domain name for the IP address is inserted in the *Received* header field. If the process is unsuccessful, only the IP address is included.

Note Because this feature verifies addresses for all incoming messages, its use could affect Microsoft SMTP Service performance.

Enable Logging

You can use transaction logging to track individual message transactions, including time of receipt. You can choose one of the four logging formats Microsoft SMTP Service uses to record information by selecting a format from the list. Transaction logging is enabled by default, and the format used is the W3C Extended Log File Format.

Note Because this feature tracks all transactions, its use may affect Microsoft SMTP Service performance.

Badmail Directory

When a message is undeliverable, it is returned to the sender with a non-delivery report (NDR). You can designate that copies of the NDR are sent to a location of your choice.

All NDRs go through the same delivery process as other messages, including attempts to resend the message. If the NDR has reached the retry limit and cannot be delivered to the sender, a copy of the message is placed in the Badmail directory. Messages placed in the Badmail directory cannot be delivered or returned. Check the directory regularly and reconcile the messages, because a full directory may adversely affect Microsoft SMTP Service performance.

Operators

In addition to determining which computers have access to the SMTP site and whether Transport Layer Security (TLS) is required for incoming connections, you can designate which client accounts can have operator permissions for the site. Any existing Windows NT Server account can be granted access permissions for the site by selecting it from a list. These permissions can be rescinded by removing the account from the list of site operators.

Note This feature is available in Internet Service Manager only, not Internet Service Manager (HTML).

 SMTP Site Operators

SMTP Site Operators

You can assign operator permissions for the SMTP site to any Windows NT Server account.

Secure Communication

For computers allowed access to the SMTP site, you can require that Transport Layer Security (TLS) be used for all transmissions sent to the server. Clients can then use TLS to submit encrypted messages to Microsoft SMTP Service, which Microsoft SMTP Service can then decrypt.

IP Address and Domain Name Restrictions

You can grant or deny access to an SMTP site according to IP address. By default, all IP addresses can access sites. Administrators can either grant or deny access to a specific list of IP addresses. IP addresses can be specified individually or as a group using a subnet mask, or a domain name.

DNS Lookup

To grant or deny access for a computer, type the DNS name.

IP Address

To grant or deny access for a computer, type the IP address.

Domain Name

To grant or deny access for a computer, type the domain name.

Group of Computers

You can grant or deny access for a group of computers by typing a network address ID. If there is a subnet for the network, type a subnet mask.

Single Computer

To grant or deny access for a computer, type the IP address or enter the DNS name.

Secure Communication

You can ensure that incoming data is encrypted by requiring the use of Transport Layer Security (TLS) between servers.

To use TLS, you must create key pairs and configure key certificates. Clients can then use TLS to submit encrypted messages to Microsoft SMTP Service, which Microsoft SMTP Service can then decrypt.

Key pairs consist of a number of bits that indicate the key's security level. You can strengthen security by increasing the encryption level from the default key strength of 40 bits to 128 bits. The larger the number of bits, the more difficult the item is to decrypt. Users attempting to secure access must use the same encryption level that you set.



[Require Secure Channel](#)



[Require 128-bit Encryption](#)



[Key Manager](#)

Key Manager

You can use the Key Manager to create new key requests and manage installed key certificates for the SMTP site.

Require 128-bit encryption

Key pairs consist of a number of bits that indicate the key's security level. You can strengthen security by increasing the encryption level from the default key strength of 40 bits to 128 bits. The larger the number of bits, the more difficult the item is to decrypt. Users attempting to secure access must use the same encryption level that you set.

Due to export restrictions, the 128-bit key strength encryption feature is available only in the United States and Canada. For information about upgrading to 128-bit encryption capability, see <http://www.microsoft.com/NTServerSupport>.

Require Secure Channel

You can ensure that incoming data is encrypted by requiring the use of Transport Layer Security (TLS) between servers.










To use TLS, you must create key pairs and configure key certificates. Client computers can then use TLS to submit encrypted messages to Microsoft SMTP Service, which Microsoft SMTP Service can then decrypt.

Key pairs consist of a number of bits that indicate the key's security level. You can strengthen security by increasing the encryption level from the default key strength of 40 bits to 128 bits. The larger the number of bits, the more difficult the item is to decrypt. Users attempting to secure access must use the same encryption level that you set.

Due to export restrictions, the 128-bit key strength encryption feature is available only in the United States and Canada. For information about upgrading to 128-bit encryption capability, see <http://www.microsoft.com/NTServerSupport>.

Delivery

Once a connection has been opened and the receiving server has acknowledged that it is ready to receive data, messages can be transmitted for delivery. You can use the **Delivery** property sheet to set all delivery and routing options. This includes setting retry intervals for delivering messages, limiting the number of hops to servers during delivery, and identifying a masquerade domain name to display in the *From* line instead of the sender's original domain name.

-  [Maximum Retries](#)
-  [Retry Interval](#)
-  [Maximum Hop Count](#)
-  [Masquerade Domain](#)
-  [Fully Qualified Domain Name](#)
-  [Smart Host](#)
-  [Attempt Direct Delivery Before Sending to Smart Host](#)
-  [Perform Reverse DNS Lookup on Incoming Messages](#)
-  [Outbound Security](#)

Fully Qualified Domain Name

There are two records that can be used to identify and verify a computer in a TCP/IP network. The mail exchanger (MX) record identifies the host and domain name associated with the computer. It uses the fully qualified domain name (FQDN) for the domain name. The address (A) record identifies the IP address for the computer. When both records are used, name resolution occurs faster.

For Microsoft SMTP Service to process MX records, an FQDN must be designated. An FQDN is used by DNS to identify the host server for a domain. The syntax is *host.domain*. For example, *CompanyA.com* may have several host servers, one of which is named *Server01*. The FQDN for the server would be *Server01.CompanyA.com*.

There are two options for specifying an FQDN for use in Microsoft SMTP Service. You can use the name specified in the **DNS** property sheet for the TCP/IP protocol in the Network application in Control Panel. Alternatively, you can specify a unique FQDN for the site.







At startup, the name designated in the **DNS** property sheet for the TCP/IP protocol in the Network application in Control Panel is automatically used for the FQDN. If you change the name in the **DNS** property sheet, the new name is automatically used for the FQDN when the service is next started. No action is required to update the FQDN for the site. This name is also used for the default domain.

To override the automatic use of the network domain, name the FQDN in the **Delivery** property sheet. Microsoft SMTP Service can then use the designated name instead of the network domain.

For more information on FQDNs, see your Windows NT Server documentation.

Messages

Once a connection has been opened and the receiving server has acknowledged that it is ready to receive data, messages can be transmitted for delivery. You can use the **Messages** property sheet to determine transmission requirements and limits.

-  [Maximum Message Size](#)
-  [Maximum Session Size](#)
-  [Maximum Number of Outbound Messages per Connection](#)
-  [Maximum Number of Recipients per Message](#)
-  [Send a Copy of Non-delivery Report To](#)
-  [Badmail Directory](#)

Maximum Hop Count

When a message is delivered, it may be routed to a number of servers before reaching its final destination. You can designate how many servers the message is allowed to pass through. This is referred to as the *hop count*.

After the hop count is set, the SMTP server counts hops listed in the *Received* header lines of the message header. When the number of *Received* fields exceeds the maximum hop count setting, the message is returned to the sender with a non-delivery report (NDR). The default is 15 hops.

Maximum Message Size

There are two related message size limit settings. The **Maximum message size** is a preferred limit for the server. If a mail client sends a message that exceeds the limit, the message is still processed as long as it does not exceed the **Maximum session size**. The **Maximum session size** is an absolute. A connection is automatically closed if a message reaches this limit.

For the **Maximum message size**, type a value for the maximum size of a message, in kilobytes (KB). The default is 2048 KB. The minimum value is 1KB.

Maximum Session Size

If the size of a message reaches the limit designated in the **Maximum session size** text box, the connection is automatically closed.

Type a value to indicate the maximum size in kilobytes (KB) a message can be before the connection closes. This number will always be larger than the **Maximum message size** and should be set carefully, because the connecting message transfer agent (MTA) is likely to resubmit the message repeatedly. The default size is 10240 KB. The minimum value is equal to the **Maximum message size**.

Maximum Retries

If a message cannot be delivered on the first attempt, it is sent again from the Queue directory after a specified time. For both the local and remote queues, you can designate the number of times to attempt to deliver a message and the interval between each attempt. After the limit is reached, the message is returned to the sender with a non-delivery report (NDR) and copies of the NDR are sent to the designated location, if you enable the option. The NDR is placed in the Queue directory and goes through the same delivery process as messages. When the NDR reaches the maximum number of retry attempts, the NDR and message are sent to the Badmail directory.

Type a value for the number of deliveries that should be attempted before the message is returned to the sender with an NDR. The default is 48 attempts for both the local and remote queues.

Retry Interval

If a message cannot be delivered on the first attempt, it is sent again from the Queue directory after a specified time. For both the local and remote queues, type a value for the time interval between retry delivery attempts. The default for both queues is 60 minutes.

Maximum Recipients per Message

This setting limits the maximum number of recipients for a single message. The default is 100, which is the maximum number specified in Request for Comments (RFC) 821. To disable this feature, clear the check box.

Some clients return messages with a non-delivery report (NDR) once an error message is received indicating that the maximum number of recipients has been exceeded. A server running Microsoft SMTP Service does not return messages with an NDR in this instance. It opens a new connection immediately and processes the remaining recipients. For example, if the recipient limit is set to 100 and a message with 105 recipients is being transmitted, the first 100 are delivered in one connection after receipt of the error message. Then a new connection is opened and the message is processed for the remaining five recipients.

Smart Host

You can route all outgoing messages for remote domains through a smart host instead of sending them directly to the domain. This allows you to route messages over a connection that may be more direct or less costly than other routes. The smart host is similar to the route domain option for remote domains. The difference is that once a smart host is designated, all outgoing messages are routed to that server. With a route domain, only messages for the remote domain are routed to a specific server.

If you set up a smart host, you can still designate a different route for a remote domain. The route domain setting overrides the smart host setting.

Type a string or an IP address to identify the smart host. If you use an IP address, enclose it in brackets to increase system performance. Microsoft SMTP Service checks first for a string, then an IP address. The brackets identify the value as an IP address, so the string analysis is bypassed.

Attempt Direct Delivery Before Sending to Smart Host

When this is selected, Microsoft SMTP Service attempts to deliver remote messages locally before forwarding them to the smart host server. The default is to send all remote messages to the smart host, not to attempt direct delivery.



Send a Copy of Non-delivery Report To

When a message is undeliverable, it is returned to the sender with a non-delivery report (NDR). You can designate that copies of the NDR are sent to a specific mailbox. Type an e-mail address for the mailbox.

Masquerade Domain

The masquerade domain name replaces the local domain name listing in *From* lines in the message header or *Mail From* lines in the protocol.

Logging

-  Enable logging
-  Active log format

Enable Logging

You can use transaction logging to track individual message transactions, including time of receipt. You can choose one of the four logging formats Microsoft SMTP Service uses to record information by selecting a format from the list. Transaction logging is enabled by default, and the format used is the W3C Extended Log File Format.

Note Because this feature tracks all transactions, its use may affect performance.

Active Log Format

You can choose one of four logging formats to track message transactions. The Microsoft Internet Information Server (IIS) Log Format is a fixed ASCII format. The W3C Extended Log File Format is an ASCII format that can be customized and is the default option. You can choose the items you want to track. The National Center for Supercomputing Applications (NCSA) Common Log File Format is a fixed ASCII format. The ODBC logging format uses an ODBC-compliant database to store logged data for a fixed set of data fields.

Domain Properties

The SMTP site has at least one domain: the default local domain. You can add more domains and configure them as local or remote. You can delete any domain that you create, but you cannot delete the default domain.

-  [Domain Name](#)
-  [Local Domain](#)
-  [Default Local Domain](#)
-  [Alias Local Domain](#)
-  [Drop Directory](#)
-  [Remote Domain](#)
-  [Route Domain](#)
-  [Allow incoming mail to be relayed to this domain](#)
-  [Outbound Security](#)

Domain Name

The domain name varies by type of domain.

Local domain names cannot include an asterisk (*). For the default local domain you can use the domain specified in the **DNS** property sheet in the Network application in Control Panel, which is automatically assigned at startup. Or, you can type a unique name in this field to override the automatic setting.

For remote domains, you can include an asterisk (*) in the name only if it is the first character listed and is followed by a period (.). This indicates that all inclusive domains for the domain you're creating use the same settings.

For more information and guidelines, see the specific domain type listing.

Local Domain

A *local domain* is a DNS domain that is serviced by the local SMTP server. Any incoming message with a local domain name must be delivered locally to the Drop directory for the default domain or returned to the sender with a non-delivery report (NDR). Local domains are sometimes referred to as *service domains* or *supported domains*. E-mail addresses with local domain names are often referred to as *local addresses*.

You can create a default domain or an alias domain. The default domain is used to stamp message headers that lack a domain specification. Alias domains are aliases of the default domain. Messages received for an alias domain are stamped with the default domain and are placed in the Drop directory. If you add a domain and assign it as the new default, the previous default changes to an alias domain.

Default Local Domain

The default domain is used to stamp messages from addresses that do not have a domain. An SMTP site has one default domain. It cannot be deleted.

To name a default domain, you can use the name specified in the **DNS** property sheet for the TCP/IP protocol in the Network application in Control Panel as the default domain. This domain name is also used for all other services. Alternatively, you can specify a unique domain to serve as the default for Microsoft SMTP Service only.

At startup, the name designated in the **DNS** property sheet for the TCP/IP protocol in the Network application in Control Panel is automatically used for the default domain. If you change the name in the **DNS** property sheet, the new name is automatically used for the default domain when the service is next started. No action is required to update the default domain for Microsoft SMTP Service.

To override the automatic use of the network domain, name the default domain in the **Domain Properties** property sheet. Microsoft SMTP Service can then use the designated name instead of the network domain.

Alias Local Domain

You can set up alias local domains that use the same settings as the default domain. Messages received by Microsoft SMTP Service for the alias local domain are stamped with the default domain name and placed in the Drop directory designated for the default domain.

Drop Directory

All incoming local messages are delivered to the Drop directory set for the default domain. There are no mailboxes.

Any alias domain you create uses the same Drop directory. You can designate any directory as the Drop directory, provided it is local to the drive for Microsoft SMTP Service and is not already assigned as the Pickup directory. By default, this is a subdirectory of the Mailroot directory.

Remote Domain

You can set unique delivery requirements for a specific remote domain by adding a domain and configuring it accordingly. For example, you can set a predetermined delivery route, require authentication, and require that TLS be used on all connections to the domain. If the remote domain is not specifically configured, Microsoft SMTP Service will not perform any of these special operations when delivering to this domain. It will, however, complete a normal DNS lookup.





You can include an asterisk (*) in a remote domain name provided it is the first character listed and is followed by a period (.). Using the wildcard indicates that all inclusive domains for the domain you're creating use the same settings.

Route Domain

You can specify a delivery path to the domain that may be faster and less expensive than a direct link. Type the name of the server you would like to route messages through for this remote domain. This setting overrides the smart host setting in the **Delivery** property sheet.

Directory Security

Site access protection is available on several levels. You can grant or deny access for specific computers, networks, or user accounts. To prevent processing of unwanted mail, you can also block relay access to the site. For computers allowed access, you can require that Transport Layer Security (TLS) be used for all transmissions sent to the server. You can also set authentication requirements for incoming connections. You can choose how secure you want the site to be and use the **Directory Security** property sheet to obtain the level of protection needed.

-  [Anonymous Access and Authentication Control](#)
-  [Secure Communications](#)
-  [IP Address and Domain Name Restrictions](#)
-  [Relay Restrictions](#)

Select Administrator Account

Use the **Select Administrator Account** dialog box to add Windows NT Server accounts and groups to the list of site operators.

-  List Names From
-  Names
-  Add
-  Members
-  Search
-  Add Names

Add Names

Lists the user and group names that you want to add as operators. You can add a name to this list by selecting it from the **Names** box and choosing **Add**.

Search

Displays the **Find Account** dialog box, which is used to locate the user or group name that you want add.

Members

Displays the **Local Group Membership** dialog box, which lists the members of the group selected in the **Names** box.

Add

Copies the name selected in the **Names** box to the **Add Names** box.

Names

Lists the names in the domain selected in the **List Names From** box.





List Names From

Displays the domain name. Choose the down arrow to display a list of available domains.

Outbound Security

You can configure the SMTP site to provide the authentication credentials required by a receiving server. You can also require that messages are encrypted using Transport Layer Security (TLS). These options can be set for all outgoing messages on the **Delivery** property sheet, and overridden for a specific remote domain on the **Domain Properties** property sheet. This enables you to set the site authentication and encryption level to handle most of the transmissions, while allowing exceptions for individual addresses.

The authentication method you choose depends on your site configuration. If messages are commonly sent to multiple addresses, disable authentication for the site. If attempts to deliver messages to an address fail because of authentication requirements, add a remote domain for the address. Then enable authentication for the domain at the same level required by the receiving server. If messages are commonly sent to one address which requires authentication (such as a smart host), determine what level of authentication is required. Then set authentication for the site at the same level. Use the remote domain authentication settings to handle any differences.

-  [No Authentication or Encryption](#)
-  [Clear Text Authentication](#)
-  [Windows NT Challenge/Response authentication and encryption](#)
-  [TLS encryption](#)

SASL/AUTH Account

Type the account name and password of the computer you're connecting to.

Windows NT Account

Type the Windows NT account name, domain, and password of the computer you're connecting to.

Anonymous Access and Authentication Control

You can require authentication for incoming messages. There are three options available. All are selected by default so computers using no authentication, basic (clear-text) authentication, or Windows NT Challenge/Response can be authenticated. You can change the settings to achieve the level of protection needed.

Authentication Methods

You can require authentication for incoming messages. There are three options available. All are selected by default. For anonymous access, no name or password is required for incoming messages. By selecting this option and clearing the remaining two, you can disable authentication for the site. For basic authentication, an account name and password is transmitted in clear text. You specify a Windows NT Server domain that is appended to the account name for authentication. For Windows NT Challenge/Response, an account name, Windows NT Server domain name, and password are authenticated using Windows NT Challenge/Response.

Basic Authentication Domain





Designate a Windows NT Server domain to be used as the default domain for basic authentication for incoming messages. This domain name is appended to the account name. This default domain may differ from the Microsoft SMTP Service default domain, depending on your configuration. For more information, see the online documentation for Microsoft SMTP Service.

IP Address and Domain Name Restrictions

You can grant or deny access to an SMTP site according to IP address. By default, all IP addresses can access sites. Administrators can either grant or deny access to a specific list of IP addresses. IP addresses can be specified individually or as a group using a subnet mask, or a domain name.

Find Account

Helps you locate a Windows NT account. You can search all domains or specific domains.

-  [Find User or Group](#)
-  [Search All](#)
-  [Search Only In](#)
-  [Search Results](#)

Find User or Group

Type the user or group name you want to locate and choose **Search**. The **Search Results** box displays the user or group names matching your entry.

Search

Starts the search for the entry you type in the **Find User or Group** box and displays the names matching your entry in the **Search Results** box.

Search All

Choose this option to search all organization domains for the user or group name you specified in the **Find User or Group** box.

Search Only In

Choose this option to search for the user or group name you typed in the **Find User or Group** box only in the domains you select. To select more than one domain, press and hold CTRL while choosing the appropriate domains.

Search Results

Displays the user or group names matching your entry in the **Find User or Group** box.

No Authentication or Encryption

Select this option to disable authentication for outgoing messages. This is the default option.

Clear Text Authentication

Select this option to transmit the account name and password of the server you're connecting to in clear text. An account name and password are required for this option. This setting should match the receiving server's incoming authentication requirements.

Windows NT Challenge/Response Authentication and Encryption

Select this option to use Windows NT Challenge/Response for authentication. A Windows NT account name, domain, and password are required for this option. This setting should match the receiving server's incoming authentication requirements.

TLS Encryption

Select this check box to encrypt outgoing messages using Transport Layer Security (TLS). The receiving server must be able to use TLS to decrypt the messages.

The setting for this option on the **Delivery** property sheet affects all outgoing messages for the SMTP site. You can override this option for a specific remote domain by selecting or clearing the **TLS encryption** check box under **Outbound Security** on the **Domain Properties** property sheet. For example, if you do not want to use TLS for all transmissions, but send messages regularly to a remote site that requires the use of TLS for all incoming transmissions, you can clear the **TLS encryption** check box on the **Delivery** property sheet. Then you can create a remote domain for the remote site and select the **TLS encryption** check box under **Outbound Security** on the **Domain Properties** property sheet.

Outbound Security

You can configure the SMTP site to provide the authentication credentials required by a receiving server. There are two types of authentication available - clear text and Windows NT Challenge/Response. With the clear text option, the account name and password of the server you're connecting to is transmitted in clear text. The Windows NT Challenge/Response option requires a Windows NT account name, domain, and password. You can also disable authentication, which is the default option.

To require that all outgoing messages are encrypted using Transport Layer Security (TLS), select the **TLS encryption** check box.

The authentication and TLS options set on the **Delivery** property sheet can be overridden for a specific remote domain. For the domain, change the settings under **Outbound Security** on the **Domain Properties** property sheet. This enables you to set the site authentication level to handle most of the transmissions, while allowing exceptions for individual addresses.

The authentication method you choose depends on your site configuration. If messages are commonly sent to multiple addresses, disable authentication for the site. If attempts to deliver messages to an address fail because of authentication requirements, add a remote domain for the address. Then enable authentication for the domain at the same level required by the receiving server. If messages are commonly sent to one address which requires authentication (such as a smart host), determine what level of authentication is required. Then set authentication for the site at the same level. Use the remote domain authentication settings to handle any differences.

Type

Select the type of address (IP address or domain name) for which you want to deny or grant access. Depending on the type of address you select, different options appear.

Use **Single Computer** to select a single computer by IP address. Choose **DNS Lookup** to look up an IP address.

Use **Group of Computers** to select a group of computers within a subnet.

Use **Domain Name** to select all of the computers in a domain by domain name. (This option adds processing overhead and might reduce Microsoft SMTP Service performance.)

Relay Restrictions

To grant global relay access through the site, choose **Allowed to relay**. To deny global relay access, choose **Not allowed to relay**. Choose **Add** to designate exceptions by specifying a computer IP address. By default, all computers are blocked from relay access except those that have met authentication requirements.

Relay Restrictions

By default, Microsoft SMTP Service blocks computers from relaying unwanted mail through the site. You can enable relay access to the site for specific computers or for those that meet authentication requirements. The site relay access setting can be overridden for a specific remote domain.

Allow incoming mail to be relayed to this domain

By default, Microsoft SMTP Service blocks computers from relaying unwanted mail to the remote domain. You can select **Allow incoming mail to be relayed to this domain**. This setting overrides the site relay access setting.

