



TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive

Search for

[ISA Server TechCenter Home](#)

[ISA Server 2004](#)

[Technical Library](#) ▶

[Functionalities](#) ▶

[Downloads](#)

[Events & Errors](#)

[Community](#)

[Webcasts](#)

[Virtual Labs](#)

#### Product Versions

[ISA Server 2006](#)

[ISA Server 2004](#)

[ISA Server 2000](#)

#### Additional Resources

[ISA Server 2004 Developer Center](#)

[ISA Server 2004 Support Center](#)

[ISA Server Product Evaluation](#)

[TechNet Home](#) > [Products & Technologies](#) > [Servers](#) > [ISA Server TechCenter Home](#) > [ISA Server 2004](#) > [Technical Library](#) > [Planning, Deployment, and Integration](#)

# Outlook Web Access Server Publishing in ISA Server 2004 Enterprise Edition

## Microsoft Internet Security and Acceleration Server 2004

Published: January 29, 2005

### On This Page

↓ [Introduction](#)

↓ [Scenarios](#)

↓ [Solutions](#)

↓ [Additional Information](#)

## Introduction

Microsoft® Internet Security and Acceleration (ISA) Server 2004 Enterprise Edition and Microsoft Outlook® Web Access work together, to enhance security for Outlook Web Access servers. This document describes how to securely publish Outlook Web Access servers with mail server publishing rules. It describes the concepts and provides step-by-step instructions for configuring Outlook Web Access solutions.

## Outlook Web Access and ISA Server

Outlook Web Access provides Web browser access to e-mail, scheduling (including group scheduling), contacts, and collaborative information stored in Microsoft Exchange Storage System folders. Outlook Web Access is used by remote, home, and roving users.

When you publish Outlook Web Access servers through ISA Server, you are protecting the Outlook Web Access server from direct external access because the name and IP address of the Outlook Web Access server are not accessible to the user. The user accesses the ISA Server computer, which then forwards the request to the Outlook Web Access server according to the conditions of your mail server publishing rule.

Further, ISA Server enables you to easily configure forms-based authentication and to control e-mail attachment availability, to protect your corporate resources when accessed through Outlook Web Access. For more information about forms-based authentication, see Forms-Based Authentication in this document. For more information about controlling e-mail attachment availability, see Controlling Attachment Availability in this document.

The ISA Server Outlook Web Access publishing feature also enables you to publish Outlook Mobile Access and Exchange ActiveSync®. Outlook Mobile Access provides users with access to Outlook from mobile devices. Using Exchange ActiveSync, you can synchronize with high levels of security, directly to your Exchange mailboxes from Microsoft Windows Mobile™-based devices, such as [Windows Mobile 2003 Software for Pocket PC](#), including Pocket PC Phone Edition, and [Windows Mobile 2003 Software for Smartphone](#).

## Network Load Balancing

You can use the Network Load Balancing (NLB) functionality of ISA Server to configure and manage the NLB functionality of Microsoft Windows Server™ 2003 running on ISA Server arrays.

When you configure NLB through ISA Server, NLB is integrated with ISA Server functionality. This provides important functionality that is not available in Windows NLB alone:

- NLB configuration is performed through ISA Server Management.
- ISA Server provides NLB health monitoring, and discontinues NLB on a particular computer as necessitated by its status. This prevents the continued functioning of NLB when the state of the computer does not allow the passage of traffic. For example, if there is a failure of the network adapter on the computer, or if you stop the Microsoft Firewall service, ISA Server stops NLB-directed traffic from passing through that computer. When the issue is resolved, ISA Server will again allow NLB traffic to pass through that computer.
- ISA Server works with Windows NLB to automatically configure bidirectional affinity, and does so for multiple networks. This guarantees that traffic is handled in both directions by the same array server. This is particularly important in Outlook Web Access, because it ensures that the client communicates with the same ISA Server array member for a particular session, so that the client's cookie is recognized by ISA Server.

## Web Listeners

All incoming Outlook Web Access requests must be received by a Web listener. A Web listener may be used in multiple Outlook Web Access publishing and Web publishing rules.

When you configure a Web listener, you are specifying:

- The network corresponding to the network adapter on the ISA Server computer that will listen for incoming Web requests. The Web listener can listen on all the Internet Protocol (IP) addresses associated with a network or on specific IP addresses.

### Important

You may want to publish Outlook Web Access using NLB in your ISA Server array. We recommend that you enable NLB on the Outlook Web Access servers network, and on the External network. For the most effective use of NLB, your Web listener should listen on the NLB virtual IP address for the External network. If you configure your Web listener to listen on all of the IP addresses for the network adapters, it will listen on the virtual IP address, which will distribute requests using NLB, and on the dedicated IP addresses of the network adapters, which will not make use of NLB. The procedure for configuring NLB is described in Appendix A: Configuring NLB on the ISA Server Array in this document. The procedure for selecting the virtual IP address in a Web listener is described in Creating a mail publishing rule in this document.

- The port number that will listen for incoming requests on the selected network IP addresses. For example, you can select to listen on port 80 for HTTP requests, on port 443 for HTTPS requests, or both. In the Outlook Web Access scenario, we recommend listening only for HTTPS requests, so that communication is secured by encryption.
- Client authentication methods (optional). After defining a Web listener, you can edit the Web listener properties to define authentication methods for requests, such as forms-based authentication.

## Forms-Based Authentication

Forms-based authentication is a type of authentication in which an unauthenticated user is directed to an HTML form. After the user provides credentials, the system issues a cookie containing a ticket. On subsequent requests, the system first checks the cookie to see if the user was already authenticated, so that the user does not have to supply credentials again.

Most importantly, the credential information is not cached on the client computer. This is particularly important in a scenario where users are connecting to your Outlook Web Access server from public computers, where you would not want user credentials to be cached. Users are required to reauthenticate if they close the browser, log off from a session, or navigate to another Web site. Also, you can configure a maximum idle session time-out, so that if a user is idle for a prolonged period of time, reauthentication is required.

We recommend that when using forms-based authentication, you use HTTPS for all communications with the site to prevent hackers from stealing the user's cookie. HTTPS is recommended in general for Outlook Web Access server publishing.

In a scenario involving multi-server ISA Server arrays, you must ensure that client requests for a particular session are handled by the same array member, so that the client's cookie is recognized. If the request is received by a different member, the cookie will not be recognized and the request will be dropped by that ISA Server member. An effective way to ensure that the requests are handled by the same server member is to enable integrated NLB on the ISA Server array. The procedure for enabling integrated NLB is described in Appendix A: Configuring NLB on the ISA Server Array in this document.

The procedure for configuring forms-based authentication is provided in Outlook Web Access Server Publishing Walk-through Procedure 4: Secure Outlook Web Access through the Listener in this document.

#### Notes

ISA Server supports forms-based authentication for Exchange Server 2003, Exchange 2000 Server, and Exchange Server 5.5. When you use ISA Server 2004 with Exchange Server 2003, you must choose to use forms-based authentication of only one of the products. If you use ISA Server forms-based authentication, you retain the ISA Server functionality to inspect response bodies, as well as request URLs, request headers, request bodies, and response headers. ISA Server forms-based authentication provides the additional benefits of authentication at the edge of the network and RADIUS-based authentication without domain membership. However, if you use ISA Server forms-based authentication, you cannot use the Exchange data compression feature. If you use Exchange Server 2003 forms-based authentication, ISA Server inspects request URLs, request headers, request bodies, and response headers, but does not inspect response bodies. However, you retain the Exchange data compression feature. When you use ISA Server 2004 with Exchange 2000 Server or Exchange Server 5.5, which do not provide forms-based authentication or data compression, we recommend that you use the ISA Server forms-based authentication feature. Outlook Web Access includes optional functionality that allows a user to change the password. If a user changes the password during an Outlook Web Access session, the cookie provided after the user initially logged on will no longer be valid. When forms-based authentication is configured on ISA Server, the user who changes the password during an Outlook Web Access session will receive the logon page the next time a request is made.

## Controlling Attachment Availability

Because Outlook Web Access is often used from public computers, you may want to control the user's ability to view and save attachments, so that private corporate information is not cached or saved to a public computer. ISA Server provides a mechanism for blocking e-mail attachments for users on public (shared) computers or users on private computers (or both). This prevents users from opening or saving attachments, although the attachments can be seen by the users. The procedure for blocking e-mail attachments is provided in Outlook Web Access Server Publishing Walk-through Procedure 4: Secure Outlook Web Access through the Listener in this document.

If you do not block attachments, note that some attachments, such as Windows Media® files and Excel spreadsheets, cannot be opened directly by a client connected remotely to an Outlook Web Access server. An attempt to open such a file will result in a failure of the application associated with the file. Those files must be saved locally and can then be opened. You can avoid this problem by

configuring Exchange Server 2003 or Exchange 2000 Server to force users to save attachments. This feature is not available on Exchange Server 5.5. Configuring Exchange to force the saving of attachments is described in Outlook Web Access Server Publishing Walk-through Procedure 5: Require the Saving of Attachments in Exchange in this document.

 Note

Exchange 2003 provides an attachment blocking feature, which blocks some types of files even if the feature is disabled.

[↑Top of page](#)

## Scenarios

Using Internet Security and Acceleration (ISA) Server 2004, you want to publish an Outlook Web Access server so that users can access their e-mail messages from home computers and from Internet kiosks. You want the connection to the Outlook Web Access server to be secure, and you do not want credentials or proprietary information stored on the client computers.


[↑Top of page](#)

## Solutions

The prescribed solution is to publish the Outlook Web Access server through Internet Security and Acceleration (ISA) Server 2004 using a mail server publishing rule. Communication from external clients to the ISA Server computer and from the ISA Server computer to the Outlook Web Access server will be encrypted using Secure Sockets Layer (SSL). Forms-based authentication will be enabled on the Web listener that listens for Outlook Web Access requests, and attachment availability may be controlled.

### **Publishing Outlook Web Access in ISA Server consists of these general steps:**

1. Set up the Outlook Web Access server.
2. Install the digital certificates needed to securely publish Outlook Web Access.
3. Create a mail server publishing rule to publish the Outlook Web Access server.

 Notes

We strongly recommend that you use the Mail Server Publishing Wizard to publish Outlook Web Access servers. This is because by default (with the exception of an Outlook Web Access publishing rule created with the Mail Publishing Rule Wizard), Web publishing rules do not forward the Accept-Encoding header to the published Web server. As a consequence, Web servers will not compress content returned to requesting clients.

#### 4. Configure caching.

##### Notes

When you use ISA Server forms-based authentication as recommended, no objects are cached from the Outlook Web Access server. To take advantage of the ISA Server caching feature, you can create a cache rule to enable caching of the images served by Outlook Web Access. Do not enable caching of other objects, because this can lead to unexpected logging off of users.

If you do not use ISA Server forms-based authentication, when the ISA Server caching feature is enabled, all Outlook Web Access objects will be cached. This can lead to unexpected logging off of users. To avoid this, you must create a cache rule to prevent the caching of Outlook Web Access objects except for images.

#### 5. Set Outlook Web Access options, such as forms-based authentication and blocking of attachments for public (shared) or private computers.

##### Notes

You can also publish an Outlook Web Access server using a server publishing rule for the HTTPS protocol. This is not a recommended ISA Server Outlook Web Access publishing solution, because it requires you to publish an entire server, rather than just the specific Exchange folders required for Outlook Web Access. Further, server publishing rules do not enable you to control user authentication requirements, because the mail server publishing rules control this. Also, when you publish an Outlook Web Access server using mail server rules, you can take advantage of the added security provided by the HTTP filter. For information about server publishing rules or the HTTP filter, see the ISA Server 2004 product Help.

### Network Topology

The following computers are necessary to deploy this solution:

- A computer to serve as the Outlook Web Access server on the Internal network. The Outlook Web Access server should run Microsoft Windows Server™ 2003 or Windows® 2000 Server with Service Pack 3.
- A computer to serve as the ISA Server Configuration Storage Server.
- A minimum of two computers running ISA Server services in an array.
- A computer on the External network, to test the solution.

##### Note

You can host the Configuration Storage server on one of the computers running ISA Server services. Or, you can have a single-computer array, in which the computer running ISA Server services also hosts the Configuration Storage server. A single-computer array will not allow you to use NLB.

### Outlook Web Access Server Publishing — Walk-through

This walk-through contains the following procedures:

- Back up your current configuration
- Configure the Outlook Web Access server

- Configure the ISA Server array
- Secure Outlook Web Access through the listener
- Require the saving of attachments in Exchange
- Test the deployment
- View Outlook Web Access session information in the ISA Server logs

This walk-through assumes that you have installed a Configuration Storage server, and at least one ISA Server array, through which you are going to publish the Outlook Web Access server. Installation of these ISA Server components is described in the product documentation and in the [Getting Started Guide](http://go.microsoft.com/fwlink/?LinkId=37794) (<http://go.microsoft.com/fwlink/?LinkId=37794>).

### **Outlook Web Access Server Publishing Walk-through Procedure 1: Back Up Your Current Configuration**

We recommend that you back up your array configuration before making any changes. If the changes you make result in behavior that you did not expect, you can revert to the previous, backup configuration. To back up the complete configuration of your ISA Server computer to an .xml document, follow this procedure:

1. Open Microsoft ISA Server Management.
2. Expand **Arrays**, right-click the array through which you are going to publish Outlook Web Access, and then click **Export (Back Up)** to start the Export Wizard.
3. On the **Welcome** page, click **Next**.
4. On the **Export Preferences** page, you can select the following options:
  - You can choose to export confidential information. If you do, it will be encrypted during export. If you want to export confidential information, select **Export confidential information** and provide a password.
  - You can choose to export user permission settings, by selecting **Export user permission settings**. User permission settings contain the security roles of ISA Server users, for example, indicating who has administrative rights.
5. Click **Next**.
6. On the **Export File Location** page, provide the location and name of the file to which you want to save the configuration. Choose a meaningful name, and consider including the date in the name of the file, such as **Cleveland Array ISA Backup 15 October 2004**. Click **Next**.
7. On the **Completing the Export Wizard** page, click **Finish**.

8. When the export has completed, click **OK**.

 **Note**


Because the .xml document is being used as a backup, a copy of it should be saved on another computer in case of catastrophic failure.

## **Outlook Web Access Server Publishing Walk-through Procedure 2: Configure the Outlook Web Access Server**

Follow these steps to configure the Outlook Web Access server.

### **Installing a digital certificate on the Outlook Web Access server**

Prepare and install a digital certificate on the Outlook Web Access server as described in the document [Digital Certificates for ISA Server 2004](http://www.microsoft.com/technet/isa/2004/plan/outlook_web_access_publishing_ee.mspx) (<http://www.microsoft.com>).

 **Notes**

The recommended configuration for Outlook Web Access publishing is to use SSL-encrypted communication (HTTPS) both from the external client to the ISA Server computer and from the ISA Server computer to the Outlook Web Access server. This is because the credential information used in the authentication process must be protected, and should not be exposed even within the Internal network. For this reason, you must install digital certificates on both the ISA Server computer and the Outlook Web Access server. ISA Server does not support Outlook Web Access publishing rules that forward HTTP requests from the external client to the Outlook Web Access server as HTTPS.

If you create a publishing rule that forwards HTTPS requests from the external client to the Outlook Web Access server as HTTP, do not enable link translation.

### **Configuring IIS to support SSL-encrypted Basic authentication**

To configure Internet Information Services (IIS) to support SSL-encrypted Basic authentication, follow these steps:

1. Open the Internet Services Manager or your custom Microsoft Management Console (MMC) containing the Internet Information Services (IIS) snap-in, expand the server node, expand the **Default Web Site** node, select **virtual path /Exchange**, and then click **Properties**.
2. Click the **Directory security** tab and under **Authentication and Access Control**, click **Edit**.
3. Under **Authenticated access**, select **Basic Authentication**, and then provide the domain against which users should be authenticated. Clear **Integrated Windows authentication** if it is selected, because Basic authentication is the preferred authentication scheme.
4. Click **OK**. A dialog box will indicate that Basic authentication method is unsecured. Because you will encrypt this authentication protocol using SSL, you can click **Yes** to continue.
5. Click **OK**. A dialog box may appear, prompting you to specify how the authentication setting should propagate to child nodes in the default site. Click **Select All** and click **OK**.

6. Under **Secure Communications**, click **Edit**, select the **Require secure channel (SSL)** check box, and then click **OK** twice.

7. Repeat these steps for the virtual path **/public**.

8. Repeat these steps for the virtual path **/exchweb**, but select **Enable anonymous access** and clear all other authenticated access check boxes.

 **Important**


Exchange Server 2003 provides an option of enabling forms-based authentication. Do not select that option, because it will not work with ISA Server mail publishing rules. Forms-based authentication should be configured on the ISA Server computer.

### **Outlook Web Access Server Publishing Walk-through Procedure 3: Configure the ISA Server Array**

Follow these steps to configure the ISA Server array.

#### **Installing a digital certificate on the ISA Server array member**

Prepare and install a digital certificate on each of the ISA Server array members as described in the document [Digital Certificates for ISA Server 2004](#) (<http://www.microsoft.com>). The certificates should be identical.

 **Note**

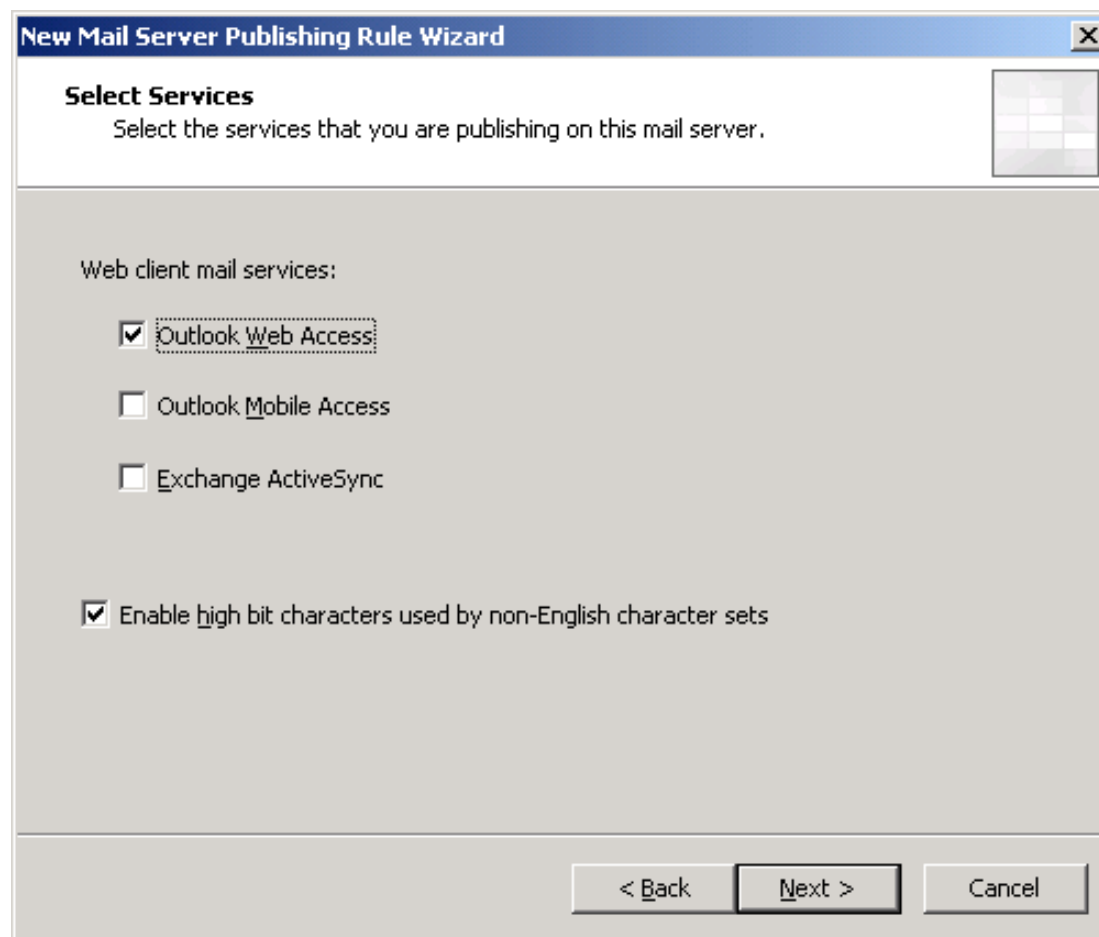
The recommended configuration for Outlook Web Access publishing is to use SSL-encrypted communication (HTTPS) both from the external client to the ISA Server computer and from the ISA Server computer to the Outlook Web Access server. For this reason, you must install digital certificates on both the ISA Server computer and the Outlook Web Access server.

#### **Creating a mail publishing rule**

Create a new mail publishing rule using the New Mail Server Publishing Rule Wizard. Follow these steps:

1. On one of the ISA Server array members, expand Microsoft ISA Server Management, expand **Arrays**, and expand the array that will publish Outlook Web Access. Click **Firewall Policy**.
2. In the Firewall Policy task pane, on the **Tasks** tab, select **Publish a Mail Server** to start the New Mail Server Publishing Rule Wizard.
3. On the **Welcome** page of the wizard, provide a name for the rule, and then click **Next**.
4. On the **Select Access Type** page, select **Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync**, and then click **Next**.

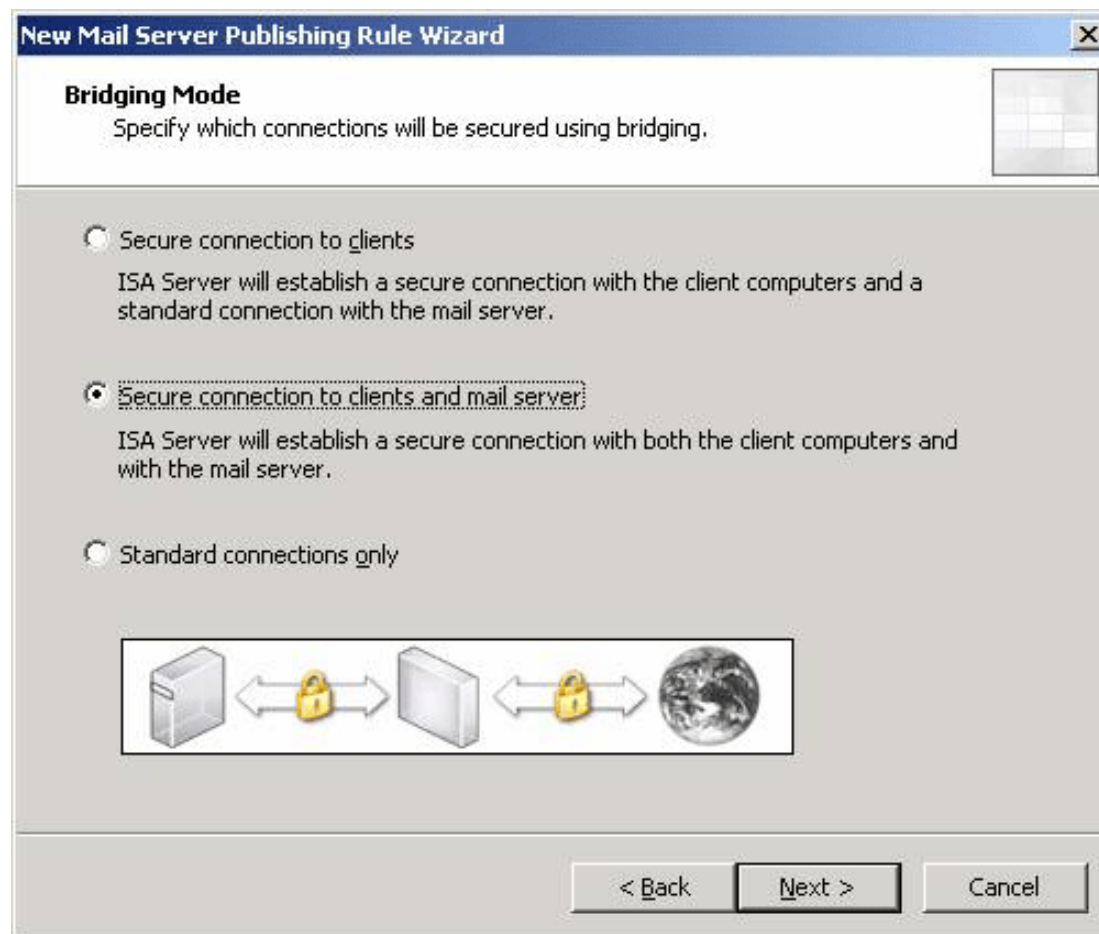
5. On the **Select Services** page, select **Outlook Web Access**. You may also select **Outlook Mobile Access** and **Exchange ActiveSync**. These services are described in Outlook Web Access and ISA Server in this document. Click **Next**.



 Note

Enable high bit characters used by non-English character sets is enabled by default. This allows DBCS or Latin 1 characters, used in some non-English languages. If you clear this selection, requests using those characters will be blocked.

6. On the **Bridging Mode** page, select which parts of the communication path will be secured by digital certificates and therefore take place using the HTTPS protocol. This can be the communication from the client to the ISA Server computer, the communication from the ISA Server computer to the Outlook Web Access server, both types of communication, or neither. We recommend that you select the default **Secure connection to clients and mail server**, so that both portions of the communications pathway are secured by digital certificates. This will require that a digital certificate be installed on the Outlook Web Access server and on the ISA Server computer, as described in the document [Digital Certificates for ISA Server 2004](http://www.microsoft.com) (<http://www.microsoft.com>). Click **Next**.



7. On the **Specify the Web Mail Server** page, enter the name or IP address of the Outlook Web Access server. This name must match the name on the Outlook Web Access server digital certificate. Click **Next**.

8. On the **Public Name Details** page, provide information regarding what requests will be received by the ISA Server computer and forwarded to the Outlook Web Access server. In **Accepts requests for**, if you select **Any domain name**, any request that is resolved to the IP address of the external Web listener of the ISA Server computer will be forwarded to your Outlook Web Access server. If you select **This domain name** and provide a specific domain name, such as **mail.fabrikam.com**, assuming that domain is resolved to the IP address of the external Web listener of the ISA Server computer, only requests for **https://mail.fabrikam.com** will be forwarded to the Outlook Web Access server. Click **Next**.



Note

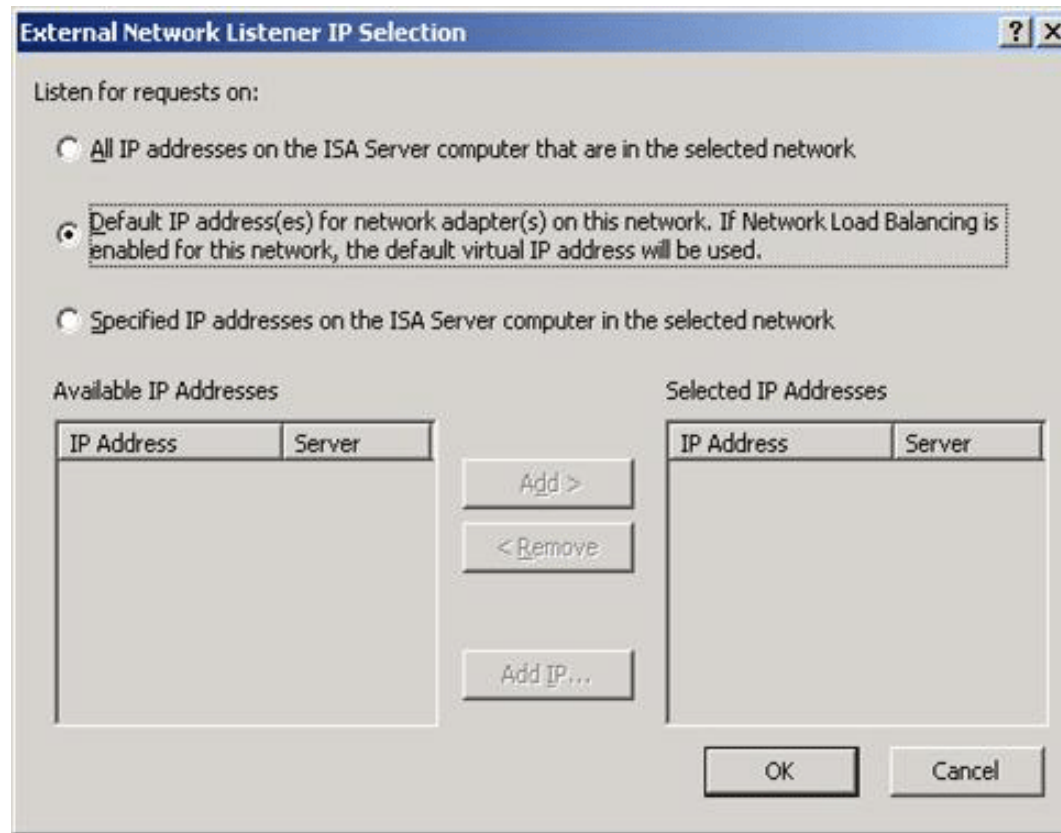
The public name must match the name of the digital certificate on the ISA Server array.

9. On the **Select Web Listener** page, specify the Web listener that will listen for Web page requests that should be redirected to your Web server, and then click **Next**. If you have not defined a Web listener, click **New** and follow these steps to create a new listener.

1. On the **Welcome** page of the New Web Listener Wizard, type the name of the new listener, such as **Listener on External network for internal Web publishing**, and then click **Next**.

2. On the **IP Addresses** page, select the network that will listen for Web requests. Because you want ISA Server to receive requests from the External network (the Internet), the listener should be one or more IP addresses on the External network adapters of ISA Server. Therefore, select **External**. Do not click **Next**.

3. Before you click **Next** on the **IP Addresses** page, select specific addresses on which you will listen. Click the **Address** button. The default selection is to listen on all IP addresses on the network. This will include both dedicated IP addresses and virtual IP addresses on the External network, where NLB is enabled. We recommend that you select **Default IP address(es) for network adapter(s) on this network**. This will select the default virtual IP address if NLB is enabled, and will select the default IP addresses on the network adapters of the ISA Server array if NLB is not enabled. If you have enabled NLB, and have created more than one virtual IP address, you should select **Specified IP addresses on the ISA Server computer in the selected network**, and then select the specific virtual IP address in the **Available IP Addresses** list.



4. Click **OK**, and on the **IP Addresses** page, click **Next**.

5. On the **Port Specification** page, the **HTTP port** is set to 80 (default setting). If you want to receive HTTPS requests, select **Enable SSL**, verify that the **SSL port** is set to 443 (default setting), and provide the certificate name in the **Certificate** field. This requires that you have a digital certificate installed on the ISA Server computer. For more information about certificates, see [Digital Certificates for ISA Server 2004](http://www.microsoft.com) (<http://www.microsoft.com>). We recommend that you install a certificate, disable the HTTP port, and enable SSL, so that only HTTPS (encrypted) communication can take place between the clients and your server. Click **Select**, select the certificate you installed, click **OK**, and then click **Next**.

**New Web Listener Definition Wizard**

**Port Specification**  
Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming Web requests.

**HTTP**

Enable HTTP

HTTP port:

**SSL**

Enable SSL

SSL port:

Certificate:

[Help about Web listener port specification](#)

< Back    Next >    Cancel

◆ Important

For secure Outlook Web Access publication, we recommend that you listen only for SSL requests. Use only the standard port numbers, which are the default settings, for Outlook Web Access publishing.

6. On the **Completing the New Web Listener Wizard** page, review the settings, and click **Finish**.

10. On the **Select Web Listener** page, click **Next**.

📌 Note

For security purposes, you should consider using forms-based authentication and limiting attachment access from public computers. These features are part of the listener used in the mail server publishing rule, but are not configured in the New Web Listener Wizard. For more information, see Outlook Web Access Server Publishing Walk-through Procedure 4: Secure Outlook Web Access through the Listener in this document.

11. On the **User Sets** page, the default, **All Users**, is displayed. This will allow any authenticated user in the External network to access the Outlook Web Access server. To restrict the access to specific users, use the **Remove** button to remove **All Users**, and the **Add** button to access the **Add Users** dialog box, from which you can add the user set to which the rule applies. The **Add Users** dialog box also provides access to the New User Sets Wizard through the **New** menu item. When you have completed the user set selection, click **Next**.
12. On the **Completing the New Mail Server Publishing Rule Wizard** page, scroll through the rule configuration to make sure that you have configured the rule correctly, and then click **Finish**.
13. In the ISA Server details pane, click **Apply** to apply the changes you have made. It will take a few moments for the changes to be applied.

### Creating a cache rule

When you use ISA Server forms-based authentication as recommended, no objects are cached from the Outlook Web Access server. To take advantage of the ISA Server caching feature, you can create a cache rule to enable caching of the images served by Outlook Web Access. Do not enable caching of other objects, because this can lead to unexpected logging off of users. The cache rule must have the following properties:

- Cache Rule Destination. Specify a URL set containing only **http://NameOfOutlookWebAccessServer/exchweb/img/\***.
- Content Retrieval. Select the option **Only if a valid version of the object exists in the cache**.
- Cache Content. Select the options **If source and request headers indicate to cache** and **Content requiring user authentication for retrieval**.
- All other properties can be left in their default condition.

If you do not use ISA Server forms-based authentication, when the ISA Server caching feature is enabled, all Outlook Web Access objects will be cached. This can lead to unexpected logging off of users. To avoid this, you must create a cache rule to prevent the caching of Outlook Web Access objects except for images. The cache rule must have the following properties:

- Cache Rule Destination. Specify a URL set containing **http://NameOfOutlookWebAccessServer/exchweb/\***. After you create the rule using the New Cache Rule Wizard, open the rule properties, and on the **To** tab, add **http://NameOfOutlookWebAccessServer/exchweb/img/\*** to the **Exceptions**. This will allow caching of the img (images) path.
- Content Retrieval. Select the option **Only if a valid version of the object exists in the cache**.
- Cache Content. Select the option **Never, no content will ever be cached**.

### To create a cache rule, follow these steps:

1. Expand Microsoft ISA Server Management, expand **Arrays**, expand the array that publishes Outlook Web Access, expand **Configuration**, and then click **Cache**.
2. In the details pane, click the **Cache Rules** tab.

3. In the task pane, on the **Tasks** tab, select **Create a Cache Rule** to start the New Cache Rule Wizard.
4. On the **Welcome** page of the wizard, provide a name for the rule, and then click **Next**.
5. On the **Cache Rule Destination** page, click **Add** to open the **Add Network Entities** dialog box, select the appropriate network entity, click **Add**, and then click **Close**. On the **Cache Rule Destination** page, click **Next**.
6. On the **Content Retrieval** page, leave the default selection **Only if a valid version of the object exists in the cache**, and then click **Next**.
7. On the **Cache Content** page, select options as described earlier in this topic.
8. You can use the default selections on the remaining wizard pages. Information about cache rule properties is provided in the product Help. Review the information on the wizard summary page, and then click **Finish**.

#### **Outlook Web Access Server Publishing Walk-through Procedure 4: Secure Outlook Web Access through the Listener**

The listener that listens for Outlook Web Access server requests (created in Procedure 3) provides these important features for securing your Outlook Web Access server:

- Forms-based authentication, described in Forms-Based Authentication in this document.
- Control of attachment availability, described in Controlling Attachment Availability in this document.

These features cannot be configured in the New Web Listener Wizard. After you have created a new Web listener in the New Web Listener Wizard, use the following steps to configure the listener to use forms-based authentication and to limit attachment availability. To secure Outlook Web Access through the listener, follow these steps:

1. In ISA Server Management, expand **Arrays**, expand the array that publishes Outlook Web Access, and select the **Firewall Policy** node. In the task pane, select the **Toolbox** tab, and then select the **Network Objects** header.
2. In the **Network Objects** header, expand **Web Listeners**. Double-click the Web listener you created for Outlook Web Access publishing to open its properties.
3. On the **Preferences** tab, under **Configure allowed authentication methods**, click **Authentication**.
4. In the list of authentication methods, clear any authentication method that is selected (the default is **Integrated**), and then select **OWA Forms-Based**. This establishes forms-based authentication for the Outlook Web Access Web listener, and for the mail server publishing rule that uses this listener. You use the steps that follow to configure idle session time-out and attachment control options.
5. Under **Configure OWA forms-based authentication**, click **Configure** to open the **OWA Forms-Based Authentication** dialog box.

6. Under **Idle Session Timeout**, configure the maximum time that clients can remain idle without being disconnected. Typically, you should configure **Clients on public machines** to have a shorter allowed idle time than **Clients on private machines**, to reduce the risk that someone will access e-mail if the user leaves the public computer and forgets to log off. Note that this is a global setting for all Web listeners.
7. Under **E-mail Attachments**, you can select to block e-mail attachments for public and private computers. Opening attachments at public Internet terminals could potentially compromise corporate security, so you may want to block that access.
8. You can select **Log off OWA when the user leaves the OWA site** if you want users to be automatically logged off when they close the Internet Explorer window, refresh the window, or navigate to another Web site. This provides another layer of security, so that if your user navigates away from the Outlook Web Access site but does not log off or close the browser, another user will not have access to corporate mail.
9. Click **OK** to close the Web listener properties. In the Firewall Policy details pane, click **Apply** to apply the changes that you made.

### Outlook Web Access Server Publishing Walk-through Procedure 5: Require the Saving of Attachments in Exchange

You can completely block attachments received through Outlook Web Access, so that the user cannot open or save any attachments. The procedure for blocking e-mail attachments is provided in Outlook Web Access Server Publishing Walk-through Procedure 4: Secure Outlook Web Access through the Listener in this document.

If you do not block attachments, note that some attachments, such as Windows Media files and Excel spreadsheets, cannot be opened directly by a client connected remotely to an Outlook Web Access server. An attempt to open such a file will result in a failure of the application associated with the file. Those files must be saved locally and can then be opened. You can avoid this problem by configuring Exchange Server 2003 and Exchange 2000 Server to force users to save attachments. This feature is not available in Exchange Server 5.5.

To force users to save attachments, configure the following registry key on the Exchange Server computer:

```
HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeWEB\OWA\Level 2FileTypes
```

This registry value specifies a set of file extensions that are potentially dangerous as attachments. Attachments matching these types will not be opened automatically. Instead, users will be prompted to save the attachments locally on their computers.

#### Note

You cannot configure Exchange Server 5.5 to require the saving of attachments.

### Outlook Web Access Server Publishing Walk-through Procedure 6: Test the Deployment

After you complete the configuration, you should test the features you configured.

#### Testing Outlook Web Access

An external client can access the Outlook Web Access server provided that it can resolve a fully qualified domain name to the external IP address of the ISA Server computer. This would usually be achieved by registering a public Internet domain name with a public DNS server that maps the Web site name to the external IP address of ISA Server. To test the deployment in a lab environment, you can specify the Web site host name resolution information using Microsoft Notepad, in the client **hosts** file located under the following path: `\system32\drivers\etc\hosts` in the Windows installation directory.

To connect to the Outlook Web Access site from the external client, type the Web address, such as **https://mail.fabrikam.com/exchange**. Be certain to specify **https** in the URL, as shown.

When you connect, you should see a logon page requesting credentials and the session type (public or private). You must provide this information before you can access your mailbox.

If you have set time-outs or blocked attachments, you can test those features by leaving the browser inactive for a period of time and then trying to access mail, and by trying to open or save attachments.

#### **Testing Outlook Mobile Access**

From a computer with Internet access, use Internet Explorer to connect to your Outlook Mobile Access DNS address and make sure that Outlook Mobile Access is working properly.

#### Note

Although Internet Explorer is not a supported client for Outlook Mobile Access, it is useful to test whether you can communicate with your Exchange front-end server.

After you successfully connect to your Exchange server using Outlook Mobile Access, verify that you can connect to your Exchange server using a supported mobile device with Internet connectivity.

#### **Testing Exchange ActiveSync**

Configure a mobile device to connect to your Exchange server using Exchange ActiveSync, and make sure that ISA Server and Exchange ActiveSync are working properly.

#### Note

You can also test Exchange ActiveSync using Internet Explorer. Open Internet Explorer, and in Address, type the URL `https://published_server_name/Microsoft-Server-Activesync`, where `published_server_name` is the published name of the Outlook Web Access server (the name a user would use to access Outlook Web Access). After you authenticate yourself, if you receive an Error 501/505 – Not implemented or not supported, ISA Server and Exchange ActiveSync are working together properly.

### **Outlook Web Access Server Publishing Walk-through Procedure 7: View Outlook Web Access Session Information in the ISA Server Logs**

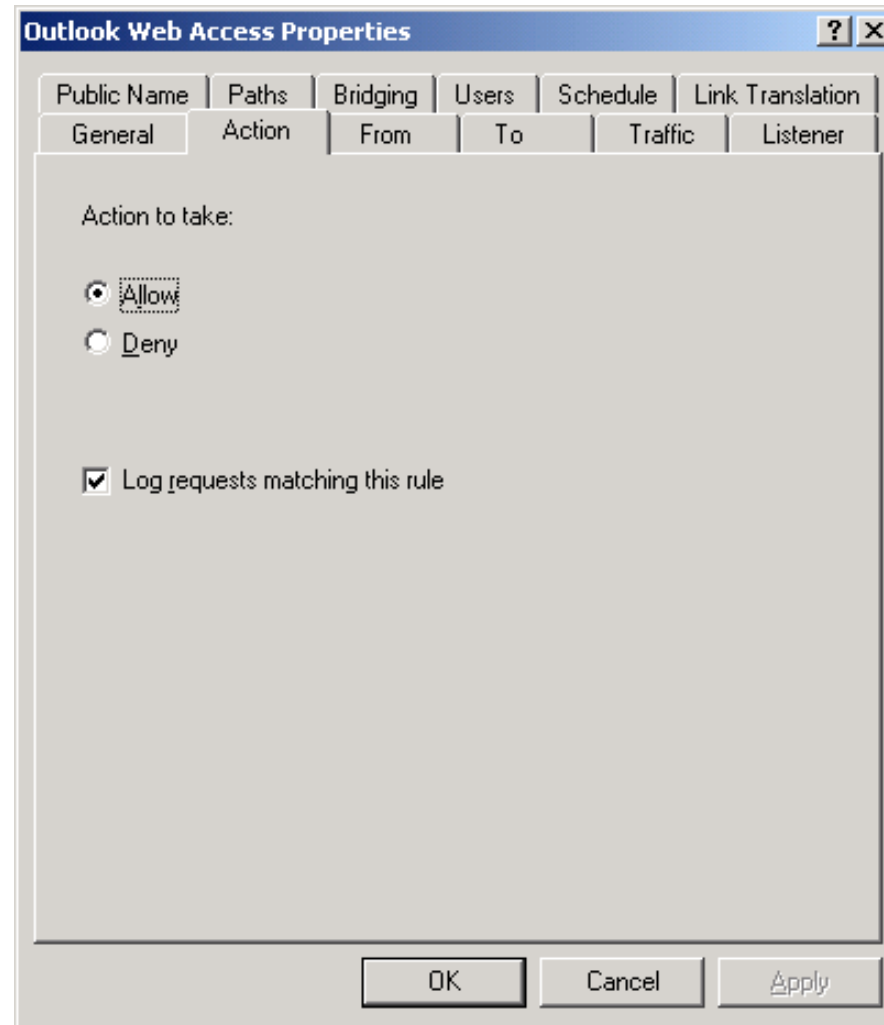
ISA Server will log the requests that match the mail server publishing rule, if **Log requests matching this rule** is selected on the **Action** tab of the rule properties. (This is the default condition.)

#### **Checking the logging property of the rule**

To check the logging property of the rule, follow these steps:

1. In the Microsoft ISA Server Management console tree, under **Arrays**, expand the array that publishes Outlook Web Access, and select **Firewall Policy**.
2. In the details pane, double-click the mail server publishing rule to open its properties dialog box.

3. Select the **Action** tab and confirm that **Log requests matching this rule** is selected.



4. Click **OK** to close the properties dialog box.

#### **Viewing the information in the log**

To view the information in the log, follow these steps:

1. In the Microsoft ISA Server Management console tree, select **Monitoring**.
2. In the Monitoring details pane, select **Logging**.

3. Create a filter so that you receive only the log information regarding Outlook Web Access access attempts. In the task pane, on the **Tasks** tab, click **Edit Filter** to open the **Edit Filter** dialog box. The filter has three default conditions, specifying that the log time is live, that log information from both the firewall and the Web Proxy should be provided, and that connection status should not be provided. You can edit these conditions, and add additional conditions to limit the information retrieved during the query.
4. Select **Log Time**. From the **Condition** drop-down menu, select **Last 24 Hours**, and then click **Update**.
5. You can add another expression by selecting an item from the **Filter by** drop-down menu, and then provide a **Condition** and **Value**. For example, to limit the log to display access to your published Web servers, you can have these expressions: **Filter by: Log Record Type, Condition: Equals, Value: Web Proxy Filter**, and **Filter by: Service, Condition: Equals, Value: Reverse Proxy**. This will limit the log to items that match Web publishing rules, including the Outlook Web Access publishing rule.
6. After you have created an expression, click **Add To List** to add it to the query list, and then click **Start Query** to start the query. The **Start Query** command is also available in the task pane on the **Tasks** tab.

## Appendix A: Configuring NLB on the ISA Server Array

Follow this procedure to configure Network Load Balancing (NLB) for an array. NLB will be automatically configured in unicast mode and single affinity. Single affinity ensures that all network traffic from a particular client be directed to the same host. This procedure takes place on a computer in an ISA Server array. You must be logged on as an array or enterprise administrator.

### To configure NLB on an ISA Server array, follow these steps:

1. On one of the ISA Server array members, expand **Arrays**, expand the array node, expand **Configuration**, and click **Networks**.
2. In the details pane, verify that the **Networks** tab is selected.
3. In the task pane, on the **Tasks** tab, click **Enable Network Load Balancing Integration** to start the Network Load Balancing Integration Wizard. On the **Welcome** page, click **Next**.
4. On the **Select Load Balanced Networks** page, select the networks for which NLB will be enabled. We recommend that you enable NLB on the Outlook Web Access servers network, and on the External network. Select those networks. Do not click **Next**.
5. Before you click **Next**, you must set the virtual IP address for each network. To set the virtual IP address, after you select the network, click **Set Virtual IP**. In the **Set Virtual IP Address** dialog box, provide the IP address and subnet mask for the virtual IP address you will use. Note that this IP address must be a valid static IP address (that cannot be assigned by your DHCP server), and must belong to the network you are configuring. Click **Next**.
6. On the summary page, click **Finish**.
7. In the details pane, click **Apply**.

[↑Top of page](#)

## Additional Information

Additional ISA Server 2004 documents are available on the [ISA Server 2004 Guidance page](http://www.microsoft.com) (http://www.microsoft.com).

## References

For information about how to deploy Outlook Web Access in Exchange Server 2003, see the [Exchange 2003 Deployment Guide](http://www.microsoft.com) (www.microsoft.com).

For information about how to deploy Outlook Web Access in Exchange 2000 Server, see the document [Outlook Web Access in Exchange 2000 Server](http://www.microsoft.com) (www.microsoft.com), and [Customizing Microsoft Outlook Web Access](http://www.microsoft.com) (www.microsoft.com).

Do you have comments about this document? Send [feedback](#).

[⤴Top of page](#)

[Manage Your Profile](#) | [Contact Us](#) | [Newsletter](#)

© 2007 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

**Microsoft**