



Deploying the BIG-IP System v10 with  
Microsoft Exchange Outlook  
Web Access 2007



**Microsoft**<sup>®</sup> Partner

---

# Table of Contents

## Deploying the BIG-IP system v10 with Microsoft Outlook Web Access 2007

Prerequisites and configuration notes .....	1-1
Product versions and revision history .....	1-2
Configuring the BIG-IP system for Outlook Web Access .....	1-3
Running the Microsoft Exchange OWA application template .....	1-3
Creating the OneConnect profile .....	1-8
Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5 .....	1-10
Modifying the HTTP profile to enable X-Forwarded-For .....	1-10
Adding the X-Forwarded-For log field to IIS .....	1-10
SSL Certificates on the BIG-IP system .....	1-12

## Manually configuring the BIG-IP LTM system

Creating the HTTP health monitor .....	2-1
Creating the pool .....	2-2
Importing keys and certificates .....	2-4
Creating profiles .....	2-5
Creating the iRules .....	2-11
Creating the virtual servers .....	2-12

## Manually configuring the WebAccelerator module with Outlook Web Access

Prerequisites and configuration notes .....	3-1
Configuring the WebAccelerator module for Outlook Web Access .....	3-1
Creating an HTTP Class profile .....	3-1
Modifying the Virtual Server to use the Class profile .....	3-3
Creating an Application .....	3-4



I

---

---

## Deploying the BIG-IP System v10 with Microsoft Exchange Outlook Web Access

---

---

- Configuring the BIG-IP system for Outlook Web Access
- Running the Microsoft Exchange OWA application template
- Creating the OneConnect profile
- SSL Certificates on the BIG-IP system

---

# Deploying the BIG-IP system v10 with Microsoft Outlook Web Access 2007

Welcome to the F5 and Microsoft® Exchange® Outlook Web Access 2007 Deployment Guide. This guide contains step-by-step procedures for configuring the BIG-IP system 10.0 for the Outlook Web Access (OWA) component of Microsoft Exchange Server.

New in version 10.0 of the BIG-IP system are Application Ready Templates. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more (requires free registration): <http://devcentral.f5.com/Default.aspx?tabid=89>.

To provide feedback on this deployment guide or other F5 solution documents, contact us at [solutionsfeedback@f5.com](mailto:solutionsfeedback@f5.com).

## Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- ◆ For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.
- ◆ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 1-12.
- ◆ To configure the Outlook Web Access servers to support SSL offloading, you must first follow Microsoft's instructions at <http://technet.microsoft.com/en-us/library/bb885060.aspx>.
- ◆ While we strongly recommend using the application template, you can manually configure the BIG-IP system. For more information, see *Manually configuring the BIG-IP LTM system*, on page 2-1.

### ◆ Important

---

*All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.*

## Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0
Microsoft Exchange Outlook Web Access	Exchange 2007 Exchange 2007 SP1

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Added optional procedure for enabling <b>X-Forwarded-For</b> on the BIG-IP LTM, and the section <i>Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5</i> , on page 1-10 for instructions on configuring IIS to log the client IP address.

---

# Configuring the BIG-IP system for Outlook Web Access

You can use the new application template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to Outlook Web Access. The template uses a set of wizard-like screens that query for information and then creates the required objects.

◆ **Note**

---

*Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.*

## Running the Microsoft Exchange OWA application template

To run the Outlook Web Access application template, use the following procedure.

### To run the Microsoft OWA application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Microsoft Exchange Outlook Web Access**. The Outlook Web Access application template opens.
4. In the Virtual Server Questions section, complete the following:
  - a) You can type a unique prefix for your OWA objects that the template will create. In our example, we leave this setting at the default, **my\_exchange\_owa**.
  - b) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step a>\_virtual\_server**. In our example, we type **192.168.14.101**.
  - c) If the servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system will use SNAT automap. See the Online Help for more information.

In our example, we leave this at the default setting: **No**.

5. In the SSL Offload section, you select the certificate and key you want to use for OWA. This template configures offloading SSL processing from your Outlook Web Access servers. To configure the OWA servers to support SSL offloading, you must follow Microsoft's instructions at [technet.microsoft.com/en-us/library/bb885060\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx)
  - a) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-12.
  - b) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-12.

For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

The screenshot shows a configuration wizard for the Microsoft Exchange Outlook Web Access Template. The breadcrumb path is 'Templates and Wizards >> Templates >> microsoft\_exchange\_owa'. The main title is 'Microsoft Exchange Outlook Web Access Template'. Below the title is a welcome message: 'Welcome to the Microsoft Exchange Outlook Web Access Template. This wizard will create a complete configuration optimized for managing Microsoft Exchange Outlook Web Access traffic.'

The 'Virtual Server Questions' section contains three questions:

- 'Unique prefix name for all objects that will be created by this template?' with the input field containing 'my\_exchange\_ow'.
- 'What IP Address do you want to use for this Microsoft Exchange OWA virtual server?' with the input field containing '192.168.14.101'.
- 'Do the Outlook Web Access servers have a route back to application clients via this BIG-IP system?' with a dropdown menu set to 'No'.

The 'SSL Offload Questions' section contains three questions:

- 'About SSL Offload:' with a text box containing: 'This template will offload SSL processing from your Outlook Web Access servers. To configure the OWA servers to support SSL offloading, you must follow Microsoft's instructions at [technet.microsoft.com/en-us/library/bb885060\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx)'.
- 'Certificate to authenticate the server? (You may need to import a certificate before deploying this Template.)' with a dropdown menu set to 'owa-ssl'.
- 'Key used for encryption? (You may need to import a key before deploying this Template.)' with a dropdown menu set to 'owa-ssl'.

**Figure 1.1** Starting the Microsoft Exchange Outlook Web Access Template

6. In the Load Balancing Questions section, complete the following:
  - a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.

- 
- b) Next, add each of the devices running OWA that are a part of this deployment.

In the **Address** box, type the IP address of the first OWA device. In our example, we type **10.132.85.101**.

In the **Service Port** box, type the appropriate port, or select it from the list. In our example, we select **HTTP** from the list. Click the **Add** button. Repeat this step for each device running OWA.

- c) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.
- d) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional.
- e) Select the HTTP version that the OWA servers expect clients to use. In our example, we select **Version 1.1**.

A new row appears asking for the fully qualified DNS name (FQDN) that clients use to access OWA. In the box, type the FQDN for your OWA deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **owa.siterequest.com**.

- f) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

Load Balancing Questions	
Which load balancing method would you like to use?	Least Connections (member)
Please add the servers that will comprise this virtual server (the virtual will not be available until at least one server is added):	Address: 10.132.85.104
	Service Port: 80 Select...
	Add
	R:1 P:1 10.132.85.101 :80 R:1 P:1 10.132.85.102 :80 R:1 P:1 10.132.85.103 :80 R:1 P:1 10.132.85.104 :80
Edit Delete	
How often should each Outlook Web Access server's health be checked?	30 seconds
HTTP request that should be sent to check server health? (HTTP 1.1 headers will be automatically added.)	GET /
What HTTP version do your Outlook Web Access servers expect clients to use?	Version 1.1
Fully qualified DNS name HTTP 1.1 clients are expected to use to access the Outlook Web Access?	owa.siterequest.c
String that should be contained within the health check response for the server to be considered healthy?	

**Figure 1.2** Configuring the Load Balancing options

7. In the Protocol and Security Questions section, complete the following
  - a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list. This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.
  - b) If you want to use the WebAccelerator module to accelerate the Outlook Web Access traffic, select **Yes** from the list. If you do not want to use the WebAccelerator, select **No**. This option does not appear if you do not have the WebAccelerator module licensed. The WebAccelerator module can significantly improve performance for OWA deployments.
  - c) If you want to use the Application Security Manager to secure the OWA traffic, select **Yes** from the list. If you do not want to use the Application Security Manager, select **No**. This option does

not appear if you do not have the Application Security Manager (ASM) licensed. For more information, see the online help or the BIG-IP ASM documentation.

- d) If you are using the Application Security Manager, from the Language Encoding list, select the appropriate language. In our example, we leave this at the default, **Unicode (utf-8)**.
- e) If you are using the WebAccelerator module, in the **Host** box, type the fully qualified DNS name (FQDN) that your users will use to access the OWA deployment (the WebAccelerator application object's Requested Hosts field). Click the **Add** button. If you have additional host names, type each one in the **Host** box, followed by clicking the **Add** button. In our example, we type **owa.siterequest.com** and click the **Add** button.

8. Click the **Finished** button.

**Protocol Optimization and Security Questions**

Will clients be connecting to this virtual server primarily over a LAN or a WAN?

Would you like to use the Web Accelerator module to accelerate your Outlook Web Access traffic?

Would you like to use the Application Security Manager module to secure your Outlook Web Access traffic?

About ASM transparent mode: Application Security Manager's policy enforcement mode will be set to transparent. In this mode, violations will be logged but not blocked. Before changing the mode to blocking, please review the log results and adjust the policy for your deployment if necessary.

What language encoding does your application use?

Please enter the fully qualified DNS names your end users will use to access the Outlook Web Access Virtual Server (e.g., owa.f5.com).

Host:

*Figure 1.3 Configuring the optimization and security options*

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created.

## Creating the OneConnect profile

One profile we recommend using for Microsoft Outlook Web Access that is not yet part of the Application template is the OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. This can provide significant performance improvements for OWA implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

In this section, we first create the OneConnect profile, then associate it with the virtual servers that were created by the Application template.

### To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The OneConnect Profile screen opens.
3. In the upper right portion of the screen, click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **owa-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

The next task is to associate the OneConnect profile you just created with the virtual server(s) that were created by the Application Template. If you are not using the BIG-IP system to offload SSL, there is only one virtual server to modify; if you are offloading SSL, there are two.

### To modify the existing OWA virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, find the HTTP virtual server that begins with the prefix you specified in step 4a. In our example, we left the prefix at the default, so we click **my\_exchange\_owa-virtual\_server**.
3. In the Configuration section, from the **OneConnect Profile** list, select the name of the profile you just created. In our example, we select **owa-oneconnect**.
4. Click the **Update** button.

---

Configuration: <span>Advanced</span>	
Type	<span>Standard</span>
Protocol	<span>TCP</span>
Protocol Profile (Client)	<span>my_exchange_owa_wan-optimized_tcp_profile</span>
Protocol Profile (Server)	<span>my_exchange_owa_lan-optimized_tcp_profile</span>
OneConnect Profile	<span>owa-oneconnect</span>

*Figure 1.4* Updating the virtual server to use the OneConnect profile

If you are using the BIG-IP system to offload SSL, repeat this procedure, but in step 2 select the HTTPS virtual server (it includes both the prefix you specified earlier, and is followed by **\_https\_**). In our example, we click **my\_exchange\_owa\_https\_virtual\_server**, and add our OneConnect profile.

## Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5

When you configure BIG-IP LTM to use SNAT, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address (in the case of SNAT **Automap**), or an address you have configured in a SNAT pool. As a result, Microsoft IIS logs each connection with its assigned SNAT address, rather than the address of the client. By configuring an HTTP profile on the BIG-IP to insert an **X-Forwarded-For** header, the original client IP address is sent as well; however, in default IIS configuration, this information is not logged.

Beginning with IIS 7, Microsoft provides an optional Advanced Logging Feature for IIS that allows you to define custom log definitions that can capture additional information such as the client IP address included in the X-Forwarded-For header.

You must first enable X-Forwarded-For in the BIG-IP HTTP profile, and then add the log field to IIS.

### Modifying the HTTP profile to enable X-Forwarded-For

The first task is to modify the HTTP profile created by the application template to enable the X-Forwarded-For header.

#### To modify the HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. From the HTTP profile list, select the profile created by the template. This is either:  
**microsoft\_exchange\_owa\_http-wan-optimized-caching\_shared\_http** or  
**microsoft\_exchange\_owa\_http-lan-optimized-caching\_shared\_http**.
3. In the Settings section, on the **Insert X-Forwarded-For** row, click the **Custom** box. From the list, select **Enabled**.
4. Click the **Update** button.

### Adding the X-Forwarded-For log field to IIS

Before beginning the following procedure, you must have installed IIS Advanced Logging. For installation instructions, see [http://www.iis.net/community/files/media/advancedlogging\\_readme.htm](http://www.iis.net/community/files/media/advancedlogging_readme.htm)

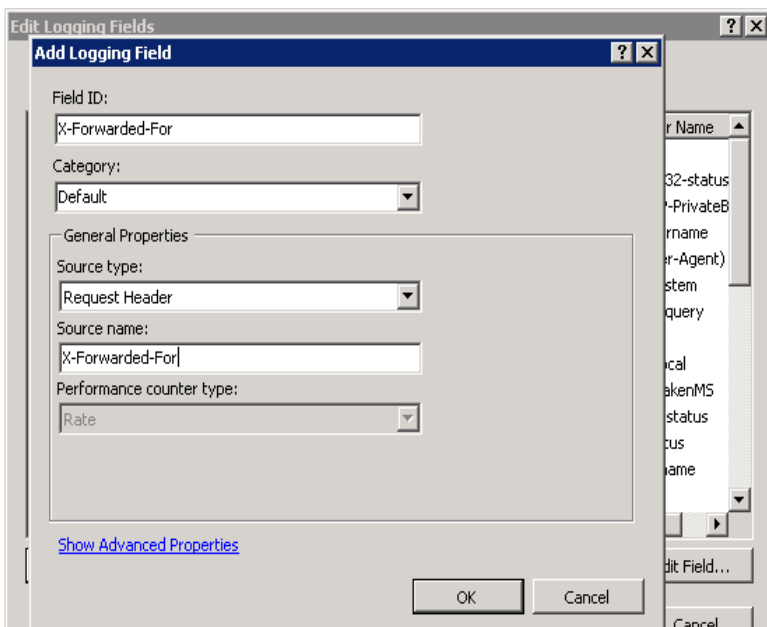
#### ◆ Note

*If you are using IIS version 6, F5 has a downloadable ISAPI filter that performs a similar function to the Advanced Logging Feature discussed here. For information on that solution, see the DevCentral post at [http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x\\_forwarded\\_for\\_log\\_filter\\_for\\_windows\\_servers.aspx](http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x_forwarded_for_log_filter_for_windows_servers.aspx)*

---

## To add the X-Forwarded-For log field to IIS

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server, web site, or directory on which you are configuring Advanced Logging. The Home page appears in the main panel.
3. From the Home page, under IIS, double-click **Advanced Logging**.
4. From the Actions pane on the right, click **Edit Logging Fields**.
5. From the Edit Logging Fields dialog box, click the **Add Field** button, and then complete the following:
  - a) In the **Field ID** box, type **X-Forwarded-For**.
  - b) From the **Category** list, select **Default**.
  - c) From the **Source Type** list, select **Request Header**.
  - d) In the **Source Name** box, type **X-Forwarded-For**.
  - e) Click the **OK** button.



*Figure 1.5 Adding the X-Forwarded-For logging field*

6. On the Connections navigation pane, return to the Computer level.
7. From the Home page, under IIS, double-click **Advanced Logging**.
8. In the Actions panel, click **Disable Advanced Logging**.
9. Click **Enable Advanced Logging**.

Now, when you look at the logs, the client IP address is included.

## SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for OWA connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

### Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

#### To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.





# 2

---

---

## Manually Configuring the BIG-IP LTM with Microsoft Outlook Web Access

---

---

- Creating the HTTP health monitor
- Creating the pool
- Importing keys and certificates
- Creating profiles
- Creating the iRules
- Creating the virtual servers

---

# Manually configuring the BIG-IP LTM system

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system rather than use the Application Template, perform the following procedures.

## Creating the HTTP health monitor

The next task is to create a health monitor for the Microsoft Outlook Web Access devices. This procedure is optional, but very strongly recommended. For this configuration, we use an HTTP monitor, which checks nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes, to not only verify that the server is up, but providing the proper content.

### To configure a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.  
In our example, we type **exch\_owa\_http**.
4. From the **Type** list, select **http**  
The HTTP Monitor configuration options appear.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91** (see Figure 2.1).
6. **Optional:** In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.  
In our example, we are using the default IIS configuration, so we use a Send String of **iisstart.htm**, and expect the Under Construction page to be returned. If you have modified the IIS configuration on the OWA servers, type a Send String and Receive Rule appropriate for your configuration.

If the page you are requesting in the Send String requires authentication, type a user name and password in the appropriate boxes.

7. Click the **Finished** button.  
The new monitor is added to the Monitor list.

Local Traffic >> Monitors >> New Monitor...

**General Properties**

Name: exch\_owa\_http

Type: HTTP

Import Settings: http

Configuration: Basic

Interval: 30 seconds

Timeout: 91 seconds

Send String: GET / isstart.htm

Receive String: [Un]der [Cc]onstruction

User Name:

Password:

Reverse:  Yes  No

Transparent:  Yes  No

Cancel Repeat Finished

*Figure 2.1 Creating the HTTP monitor*

## Creating the pool

The next step in this configuration is to create a pool on the BIG-IP LTM system for the Outlook Web Access service. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method.

### To create the OWA pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.

*Note:* For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.

- 
3. In the **Name** box, enter a name for your pool.  
In our example, we use **exch\_owa\_pool**.
  4. In the **Health Monitors** section, select the name of the monitor you created in the *Importing keys and certificates* section, and click the Add (<<) button. In our example, we select **exch\_owa\_http**.
  5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).  
In our example, we select **Least Connections (member)**.
  6. For this pool, we leave the Priority Group Activation **Disabled**.
  7. In the New Members section, make sure the **New Address** option button is selected.
  8. In the **Address** box, add the first server to the pool. In our example, we type **10.133.20.55**
  9. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list.  
In our example, we type **80**.
  10. Click the **Add** button to add the member to the list.
  11. Repeat steps 8-10 for each server you want to add to the pool.
  12. Click the **Finished** button (see Figure 2.2).

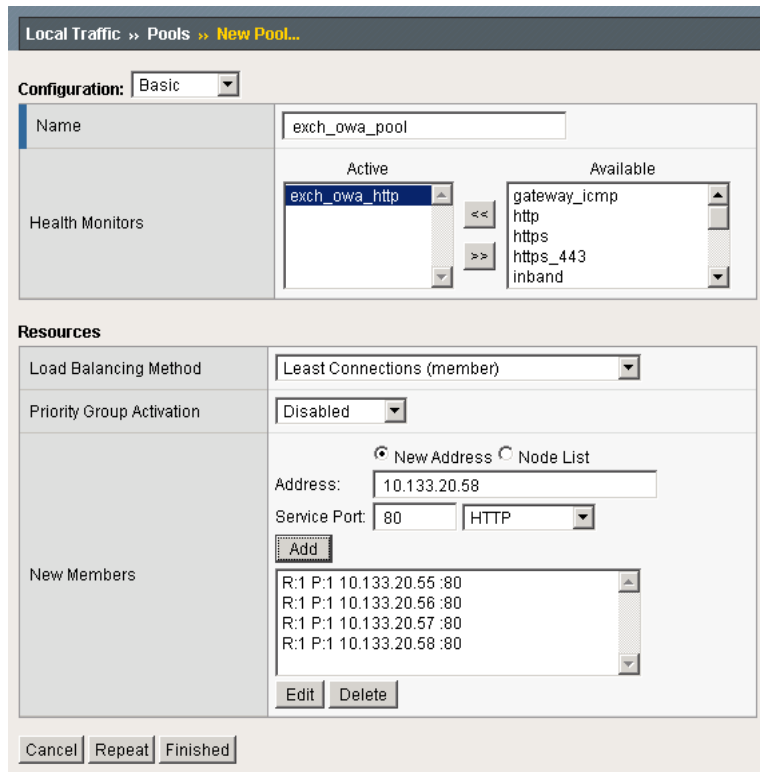


Figure 2.2 Creating the OWA pool

## Importing keys and certificates

Before you can enable the BIG-IP LTM system to offload SSL traffic from Outlook Web Access, you must install a SSL certificate and key on the BIG-IP LTM system. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM system to generate a request for a new certificate and key from a certificate authority, see the *Managing SSL Traffic* chapter in the *Configuration Guide for Local Traffic Management*.

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

### To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**.  
This displays the list of existing certificates.

- 
3. In the upper right corner of the screen, click **Import**.
  4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
  5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
  6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
  7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.

## Creating profiles

BIG-IP version 9.0 and later uses profiles. A *profile* is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP LTM system documentation.

## Creating a cookie persistence profile

The first profile we create is a persistence profile. For this configuration, we create a new cookie persistence profile, based off of the default cookie persistence profile. We use cookie persistence because users must maintain a connection to the same Outlook Web Access device.

### To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.  
The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.  
The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.  
The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_cookie**.
5. From the **Persistence Type** list, select **Cookie**.  
The configuration options for Cookie persistence appear.

6. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options.
7. Click the **Finished** button.

*Figure 2.3 Configuring Cookie persistence*

## Creating an HTTP profile

The next profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In the following example, we base our HTTP profile off of the **http-acceleration** parent profile, as we are using the WebAccelerator. If you are not using the WebAccelerator, we recommend using the **http-wan-optimized-compression-caching** parent.

### To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_http**.
4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**.
5. In the Settings section, check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Match**.

Local Traffic » Profiles : Services : HTTP » New HTTP Profile...

**General Properties**

Name	exch_owa_http
Parent Profile	http-acceleration

**Settings** Custom

Fallback Host		<input type="checkbox"/>
Fallback on Error Codes		<input type="checkbox"/>
Request Header Insert		<input type="checkbox"/>
Request Header Erase		<input type="checkbox"/>
Response Headers Allowed		<input type="checkbox"/>
Response Chunking	Selective	<input type="checkbox"/>
OneConnect Transformations	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Redirect Rewrite	Matching	<input checked="" type="checkbox"/>

**Figure 2.4** Configuring the HTTP profile

6. *Optional:* If you want to enable the X-Forwarded-For header for accurate logging, check the Custom box for **Insert X-Forwarded-For**, and from the list, select **Enabled**. See *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-10 for detailed information, including modifications to IIS to accurately log the client IP address.
7. In the Compression section, check the Custom box for **Keep Accept Encoding**, and check the box to enable Keep Accept Encoding (see Figure 2.4) Modify any of the other options as applicable for your configuration. See the online help for more information on the configuration options.
8. Click the **Finished** button.

◆ **Note**

*Some browsers and operating systems may have difficulty downloading or displaying certain compressed files. F5 suggests testing compression of each of these object types against the full range of web browsers and client operating systems in use at your organization to ensure full compatibility.*

## Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the OWA Portal users are accessing the portal via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the OWA users are accessing the system from remote or home offices, we recommend using an additional TCP profile,

called **tcp-wan-optimized** (for client side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

## Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or do not want to use this optimized profile, you can choose the default TCP parent profile.

### To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

## Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this profile.

### To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

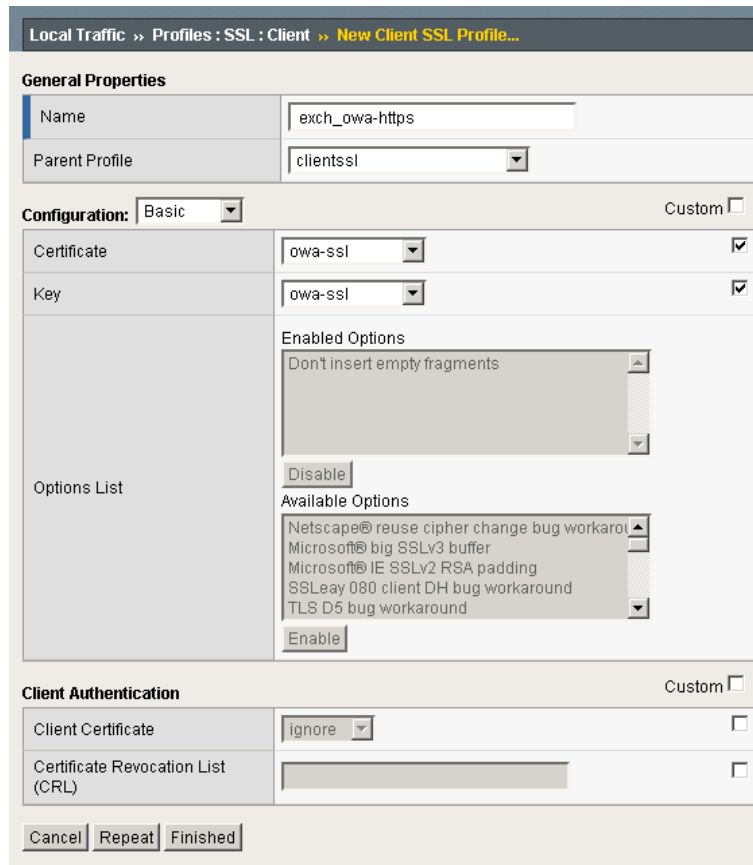
---

## Creating a Client SSL profile

The next step in this configuration is to create an SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

### To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.  
The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**.  
The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button.  
The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_https**.
6. In the Configuration section, click a check in the **Certificate** and **Key Custom** boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section (see Figure 2.5).
9. Click the **Finished** button.



*Figure 2.5 Creating the SSL profile*

## Creating the OneConnect profile

The final profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. This can provide significant performance improvements for OWA implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

### To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The OneConnect Profile screen opens.
3. In the upper right portion of the screen, click the **Create** button.

- 
4. In the **Name** box, type a name for this profile. In our example, we type **exch\_owa\_oneconnect**.
  5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
  6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
  7. Click the **Finished** button.

## Creating the iRules

In the following procedures, we create two iRules on the BIG-IP LTM system. These iRules are designed to transparently assist users in accessing Outlook Web Access if they do not properly type the correct URI. While these iRules are optional, we recommend using them as they can greatly improve end user experience.

### ◆ Note

---

*The following iRules may not be appropriate for all installations. Both iRules assume that only Exchange Server 2007 (and not previous versions) is accessible through the configured virtual server. Exchange Server 2007 Client Access Role servers can provide front-end services to both Exchange 2007 Mailbox servers and existing Exchange Server 2003 or Exchange Server 2000 back-end servers. In that case, the URIs will differ; for instance, the URI <https://<hostname>/owa/> will provide Exchange Server 2007 services, and <https://<hostname2>/exchange/> might provide services for those users still on Exchange Server 2003. For this reason, F5 recommends using a unique virtual server for each Exchange Server version being supported, in order to be able to customize each to take into account differences in the product versions. Consult the Microsoft product documentation at <http://technet.microsoft.com/en-us/library/aa998849.aspx> for more information about configuring Outlook Web Access to accommodate multiple versions of Exchange Server. For more information on advanced iRules, see <http://devcentral.f5.com/>*

## Creating the Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction. For example, this allows end users to simply type **webmail.domain.com** or <http://webmail.domain.com> without having to remember that they are going to an HTTPS URI. The rule also appends the required **/owa/** to the host portion of the URI.

### To create the Redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the **Name** box, enter a name for your iRule. In our example, we use **exch\_owa\_redirect**.
4. In the Definition section, copy and paste the following iRule:
 

```
when HTTP_REQUEST {
    HTTP::redirect https://[HTTP::host]/owa/
}
```
5. Click the **Finished** button.

## Creating the appending iRule

This iRule, which will be applied to the HTTPS virtual server, is another precautionary measure to cover the case where a user types the URI for OWA (i.e. **https://webmail.domain.com**), but forgets to add the required **/owa/** at the end. If the user did not include **/owa/**, they would likely get an Under Construction page, or another page other than their mailbox login. This iRule takes the original URI, checks to see if it has the **/owa/** portion. If it does not, the iRule adds **/owa/** automatically, transparently sending users to the correct page.

### To create the appending iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the **Name** box, enter a name for your iRule. In our example, we use **exch\_owa\_append**.
4. In the Definition section, copy and paste the following iRule:
 

```
when HTTP_REQUEST {
    if { not ([HTTP::uri] starts_with "/owa") } {
        HTTP::uri /owa[HTTP::uri]
    }
}
```
5. Click the **Finished** button.

## Creating the virtual servers

Next, we configure two virtual servers on the BIG-IP LTM system. The first virtual server is solely to intercept incoming HTTP traffic and redirect it to HTTPS using the iRule you just created. The second virtual server terminates the SSL (HTTPS) connections and sends traffic via HTTP to the pool of OWA servers.

---

## To create the HTTP virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **exch\_owa\_virtual\_http**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.20.200**.
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.

General Properties	
Name	exch_owa_virtual_http
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.20.200
Service Port	80 HTTP
State	Enabled

*Figure 2.6 Adding the Outlook Web Access virtual server*

7. In the Configuration section, select **Advanced** from the list. The Advanced configuration options appear.
8. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **exch\_owa\_tcp-wan**.
9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **exch\_owa\_tcp-wan**.
10. From the OneConnect Profile list, select the profile you created in *Creating the OneConnect profile*. In our example, we select **exch\_owa\_oneconnect**.
11. From the **HTTP Profile** list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **exch\_owa\_http** (see Figure 2.7).

The screenshot shows the 'Configuration' page with the 'Advanced' configuration mode selected. The following profiles are configured:

Type	Standard
Protocol	TCP
Protocol Profile (Client)	exch_owa_tcp-wan
Protocol Profile (Server)	exch_owa_tcp-wan
OneConnect Profile	exch_owa_oneconnect
NTLM Conn Pool	None
HTTP Profile	exch_owa_http
FTP Profile	None

**Figure 2.7** Selecting the OWA profiles

12. In the Resources section, from the **iRules** Available list, select the iRule you created for redirection in the *Creating the iRules* section. In our example, we select **exch\_owa\_httptohttps**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile* section. In our example, we select **exch\_owa\_cookie**.
14. Click the **Finished** button.

The screenshot shows the 'Resources' section of the 'Add Virtual Server' page. The configuration is as follows:

iRules	Enabled	exch_owa_append exch_owa_redirect	Available	Remove_Vary_Header _sys_auth_krbdelegate _sys_auth_ssl_cc_idap
	Up Down		Up Down	
HTTP Class Profiles	Enabled		Available	httpclass
	Up Down		Up Down	
Default Pool	+	None		
Default Persistence Profile		exch_owa_cookie		
Fallback Persistence Profile		None		

Buttons: Cancel Repeat Finished

**Figure 2.8** Resources section of the Add Virtual Server page

Now we create the virtual server for HTTPS.

---

## To create the HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.  
The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.  
The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **exch\_owa\_virtual\_https**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.20.200**.
6. In the **Service Port** box, type **443**, or select HTTPS from the list.
7. From the Configuration list, select **Advanced**.  
The Advanced configuration options appear.
8. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **exch\_owa\_tcp-wan**.
9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **exch\_owa\_tcp-wan**.
10. From the OneConnect Profile list, select the profile you created in *Creating the OneConnect profile*. In our example, we select **exch\_owa\_oneconnect**.
11. From the **HTTP Profile** list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **exch\_owa\_http** (see Figure 2.7).
12. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **exch\_owa\_https**.
13. In the Resources section, from the **iRules Available** list, select the iRule you created for appending **/owa/** to the URI in the *Creating the iRules* section. In our example, we select **exch\_owa\_append**.
14. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **exch\_owa\_pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile* section. In our example, we select **exch\_owa\_cookie**.
16. Click the **Finished** button.

This completes the manual configuration of the BIG-IP LTM system.



# 3

---

---

## Manually Configuring the WebAccelerator with Microsoft Outlook Web Access

---

---

- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

---

# Manually configuring the WebAccelerator module with Outlook Web Access

In this section, we configure the WebAccelerator module for Exchange 2007 Outlook Web Access to increase performance for end users. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

For more information on the F5 WebAccelerator, see <http://www.f5.com/products/WebAccelerator/>.

## Prerequisites and configuration notes

The following are prerequisites for this section:

- ◆ We assume that you have already configured the BIG-IP LTM system for directing traffic to the Outlook Web Access portion of Client Access, as described in this Deployment Guide.
- ◆ If you are using the WebAccelerator module, we recommend you do not configure the BIG-IP LTM system for compression or caching.
- ◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later.
- ◆ For BIG-IP version 9.4.0, you need to follow the simple procedure to download and import the policy for Outlook Web Access 2007. Later versions will include this policy.

## Configuring the WebAccelerator module for Outlook Web Access

Configuring the WebAccelerator module requires creating an HTTP class profile, creating an Application, and modifying the virtual server you created for Outlook Web Access. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the *WebAccelerator Administrator Guide* for more information.

## Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

### To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**. The HTTP Class Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Class Profile screen opens.
3. In the **Name** box, type a name for this Class. In our example, we type **exch07\_class**.
4. From the Parent Profile list, make sure **httpclass** is selected.
5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.
6. In the Hosts row, from the list select **Match Only**. The Host List options appear.
  - a) In the **Host** box, type the host name that your end users use to access Outlook Web Access. In our example, we type **owa.siterequest.com** (see Figure 3.1).
  - b) Leave the Entry Type at **Pattern String**.
  - c) Click the **Add** button.
  - d) Repeat these sub-steps for any other host names users might use to access Outlook Web Access.
7. The rest of the settings are optional, configure them as applicable for your deployment.
8. Click the **Finished** button. The new HTTP class is added to the list (see Figure 3.1).

Local Traffic » Profiles : Protocol : HTTP Class » New HTTP Class Profile...

General Properties	
Name	exch07_class
Parent Profile	httpclass

Configuration		Custom <input type="checkbox"/>
WebAccelerator	Enabled	<input checked="" type="checkbox"/>
Application Security	Disabled	<input type="checkbox"/>
Hosts	Match only...	<input checked="" type="checkbox"/>
Host List	Host: owa.siterequest.com	
	Entry Type: Pattern String	
	Add	
	<div style="border: 1px solid gray; padding: 2px;">           owa.siterequest.com         </div>	
	Delete	
URI Paths	Match all	<input type="checkbox"/>
Headers	Match all	<input type="checkbox"/>
Cookies	Match all	<input type="checkbox"/>

Actions		Custom <input type="checkbox"/>
Send To	None	<input type="checkbox"/>
Rewrite URI		<input type="checkbox"/>

Cancel Repeat Finished

*Figure 3.1* Creating a new HTTP Class profile

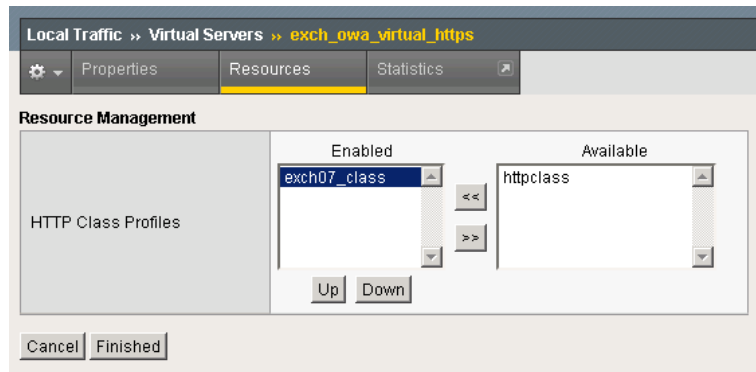
## Modifying the Virtual Server to use the Class profile

The next step is to modify the HTTPS virtual server you created in *Creating the virtual servers*, on page 2-12, to use the HTTP Class profile you just created. The HTTP profile associated with this virtual server should not have compression or RAM cache enabled, as the WebAccelerator module performs these tasks in addition to its other optimizations.

### To modify the Virtual Server to use the Class profile

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the **Virtual Server** list, click the name of the virtual server you created for your Outlook Web Access devices. In our example, we click **exch\_owa\_virtual\_https**.  
The General Properties screen for the Virtual Server opens.

3. On the Menu bar, click **Resources**.  
The Resources screen for the Virtual Server opens.
4. In the HTTP Class Profiles section, click the **Manage** button.
5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (<<) button to move it to the Enabled box. In our example, we select **exch07\_class**.
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.



*Figure 3.2 Adding the HTTP Class Profile to the Virtual Server*

## Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

### To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**. The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **New Application** button.
3. In the Application Name box, type a name for your application.  
In our example, we type **OWA 2007**.
4. In the **Description** box, you can optionally type a description.
5. From the **Local Policies** list, select **Microsoft Outlook Web Access (OWA) 2007**. This is a pre-defined policy created specifically for Outlook Web Access 2007.
6. In the **Requested Host** box, type the host name that your end users use to access Outlook Web Access. This should be the same host name you used in Step 6a in the preceding procedure. In our

---

example, we type **owa.siterequest.com**

If you have additional host names, click the **Add Host** button and enter the host name(s).

7. Click the **Save** button (see Figure 3.3).

**Configuration > Applications > New Application**

**General Options**

Application Name:

Description: (optional)

**Policies**

Central Policy:

Remote Policy:

**Hosts**

Requested Host	Action
<input type="text" value="owa.siterequest.com"/>	<a href="#">Options</a> <a href="#">Delete</a>

*Figure 3.3* Configuring an Application on the WebAccelerator

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice a marked improvement in performance after their first visit.