DEPLOYMENT GUIDE
Version 1.5

# Deploying the BIG-IP System v10 with Microsoft Office SharePoint 2007

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see https://f5.com/solutions/deployment-guides.

Microsoft® Partner

# Table of Contents

## Deploying the BIG-IP system v10 with Microsoft Office SharePoint 2007

## Manually configuring the BIG-IP LTM system with SharePoint 2007

## Manually configuring the WebAccelerator module with SharePoint 2007

1

# Deploying the BIG-IP System v10 with Microsoft Office SharePoint 2007

- Configuring the BIG-IP system for SharePoint
- Running the Microsoft SharePoint application template
- Creating the OneConnect profile
- Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5

# Deploying the BIG-IP system v10 with Microsoft Office SharePoint 2007

Welcome to the F5 and Microsoft® Office® SharePoint® 2007 Deployment Guide. This guide contains step-by-step procedures for configuring the BIG-IP system version 10.0 and later for Office SharePoint 2007, resulting in a secure, fast and available deployment.

Microsoft Office SharePoint Server 2007 enables enterprises to develop an intelligent portal that seamlessly connects users, teams, and knowledge so that people can take advantage of relevant information across business processes to help them work more efficiently.

New in version 10.0 of the BIG-IP system are Application Templates. 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***.

## 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:

- All of the configuration procedures in this document are performed on F5 devices. For information on how to deploy or configure Microsoft Office SharePoint 2007, consult the appropriate Microsoft documentation.
- 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 17.
- ***Important:*** When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the SSL virtual server and ensure correct rewriting of SharePoint site links. See *Configuring SharePoint Alternate Access Mappings to support SSL offload*, on page 1-3.

- 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 with SharePoint 2007*, 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, 10.1 |
| Microsoft Office SharePoint | SharePoint 2007 |

Revision history:

| Version | Description |
|---|---|
| 1.0 | New deployment guide |
| 1.1 | Added support for BIG-IP v10.1 |
| 1.2 | Added optional procedure for enabling **X-Forwarded-For** on the BIG-IP LTM, and the section *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-14 for instructions on configuring IIS to log the client IP address. |
| 1.3 | - Modified the optional section on using X-Forwarded-For to log the client IP address in IIS 7 and 7.5 to include installing the Custom Logging service role, and steps for editing the IIS Log Definition to include the X-Forwarded-For header .<br>- Added instructions for configuring SharePoint Alternate Access Mappings if offloading SSL on the BIG-IP system. (3-26-2012) |
| 1.4 | Added additional instructions to the Alternate Access Mappings section for ensuring the search results are properly displayed for HTTPS queries. (4-3-2012) |
| 1.5 | The original SharePoint screenshot for the Alternate Access Mappings configuration was from SharePoint 2010. Updated the screenshot for SharePoint 2007. (9-7-2012) |

# Configuring SharePoint Alternate Access Mappings to support SSL offload

If using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the BIG-IP LTM SSL virtual server and ensure correct rewriting of SharePoint site links. For SSL offload, the Alternate Access Mapping entries must have URLs defined as https://<FQDN>, where FQDN is the name associated in DNS with the appropriate Virtual Server, and assigned to the SSL certificate within the Client SSL profile.

For each public URL to be deployed behind LTM, you must first modify the URL protocol of the internal URL associated with that URL and zone from http:// to https://: and then recreate the http:// URL. If you try to just add a new URL for HTTPS, it will not function properly.

For more information, see
***http://sharepoint.microsoft.com/blog/Pages/BlogPost.aspx?pID=804***.

### To configure SharePoint Alternate Access Mappings

1. From SharePoint Central Administration navigation pane, click **Application Management**.

2. In the main pane, under Web Applications, click **Configure alternate access mappings**.

3. From the **Internal URL** list, click the Internal URL corresponding to the Public URL you want to be accessible through the BIG-IP LTM.
   The Edit Internal URLs page opens.

4. In the **URL protocol, host and port box**, change the protocol from **http://** to **https://**. You may want to make note of the URL for use in step 7.

5. Click the **OK** button. You return to the Alternate Access Mappings page.

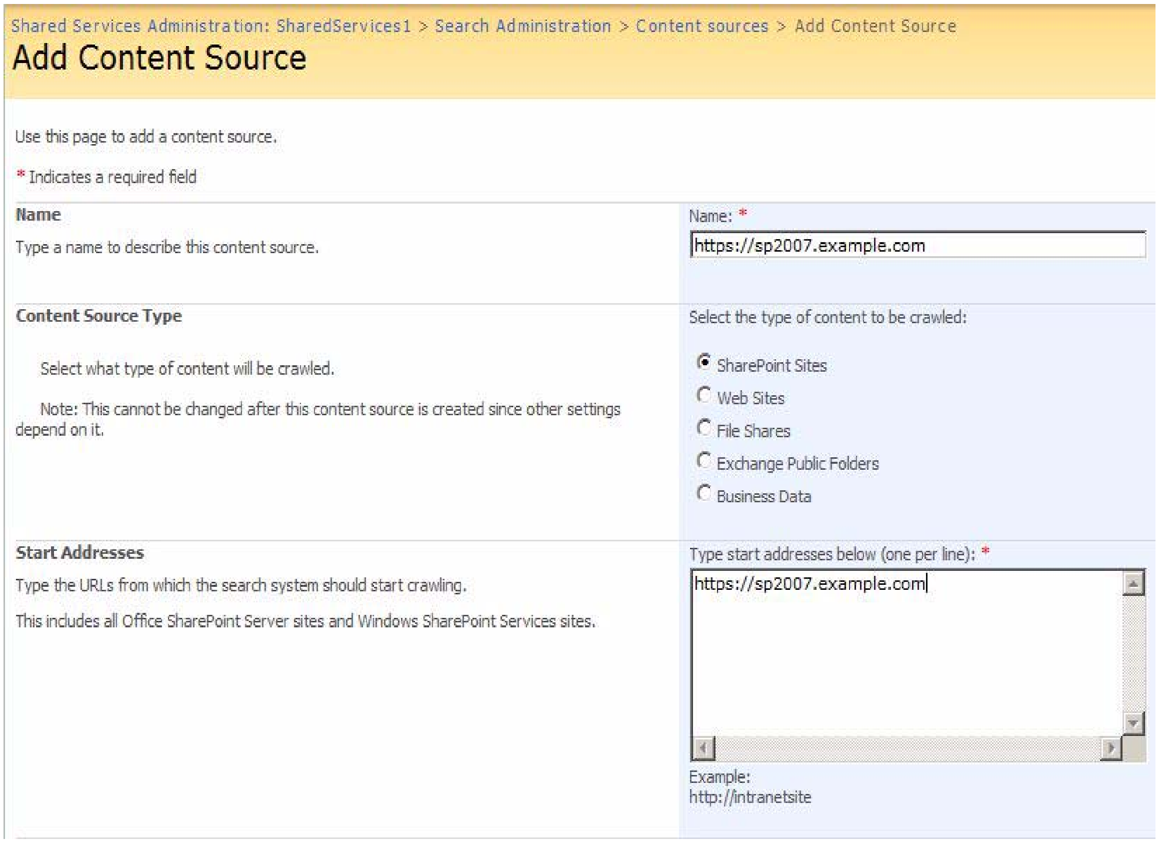
6. On the Menu bar, click **Add Internal URLs**.

7. In the **URL protocol, host and port box**, type the same internal URL used in step 4, but use the **http://** protocol. This allows access to the non-SSL site from behind the LTM.

8. Click **Save**.
   You must also add the new internal URL(s) to the list of Content Sources of Search Administration.

9. From the navigation pane, click **Application Management**, and then under **Service Applications**, click **Manage service applications**.

10. Click the name of your Search Service application. In our example, we are using Microsoft Fast Search Server, so the following examples are based on Fast Search Server.
11. In the navigation pane, click **Content Sources**.
12. On the Menu bar, click **New Content Source**.
13. In the **Name** box, type a name. We type **https://sp2007.fast.example.com**.
14. In the Start Addresses section, type the appropriate HTTPS URL. In our example, we type **https://sp2007.fast.example.com**. All other settings are optional.
15. Click the **OK** button (see Figure 1.1).
16. Repeat this entire procedure for each public URL to be deployed behind LTM.



Shared Services Administration: SharedServices1 > Search Administration > Content sources > Add Content Source

Add Content Source

Use this page to add a content source.

* Indicates a required field

**Name**

Type a name to describe this content source.

Name: *

https://sp2007.example.com

**Content Source Type**

Select what type of content will be crawled.

Note: This cannot be changed after this content source is created since other settings depend on it.

Select the type of content to be crawled:

● SharePoint Sites
○ Web Sites
○ File Shares
○ Exchange Public Folders
○ Business Data

**Start Addresses**

Type the URLs from which the search system should start crawling.

This includes all Office SharePoint Server sites and Windows SharePoint Services sites.

Type start addresses below (one per line): *

https://sp2007.example.com

Example:
http://intranetsite

***Figure 1.1*** *Adding Content Source*

## Displaying HTTPS SharePoint Search Results After Configuring Alternate Access Mappings for SSL Offloading

After configuring Alternate Access Mappings in SharePoint 2007 to support SSL offloading, you must perform the following procedure to ensure that search results are properly displayed for https:// queries. The examples below depict modifying the Content Search Service Application; however, you must also perform these steps on your Query Search Service Application.

### To ensure HTTPS search results are displayed

1. From SharePoint Central Administration navigation pane, click **Application Management**.
2. Under Service Applications, click **Manage service applications**.
3. From the Service Application list, click your Content SSA. If you are using the default content SSA, this is “Regular Search”. If you are using FAST Search, this is the name you gave the content SSA (such as FAST Content SSA).
4. From the navigation pane, under Crawling, click **Index Reset**.
5. Click the **Reset Now** button to reset all crawled content.
6. Return to your Content SSA (repeat steps 1-3).
7. From the navigation pane, under Crawling, click **Content Sources**.
8. Click the content source for which you just reset the search index.
9. From the Edit Content Source page, in the Start Full Crawl section, check the **Start full crawl of this content source** box and then click the **OK** button.

When the crawl is complete, users should receive https:// addresses in their search query results.

# Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Microsoft Office SharePoint Server 2007 deployments.

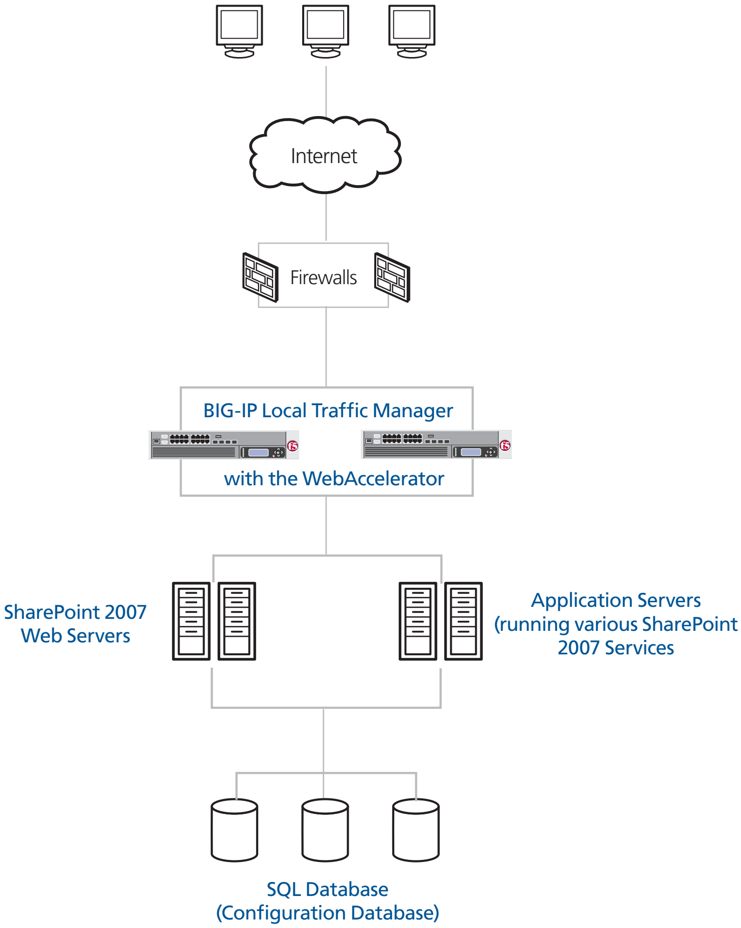


***Figure 1.2*** *Logical configuration example*

# Configuring the BIG-IP system for SharePoint

You can use the new Application Template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to Microsoft Office SharePoint. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

◆ **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 SharePoint application template

To run the SharePoint application template, use the following procedure.

### To run the Microsoft SharePoint application template

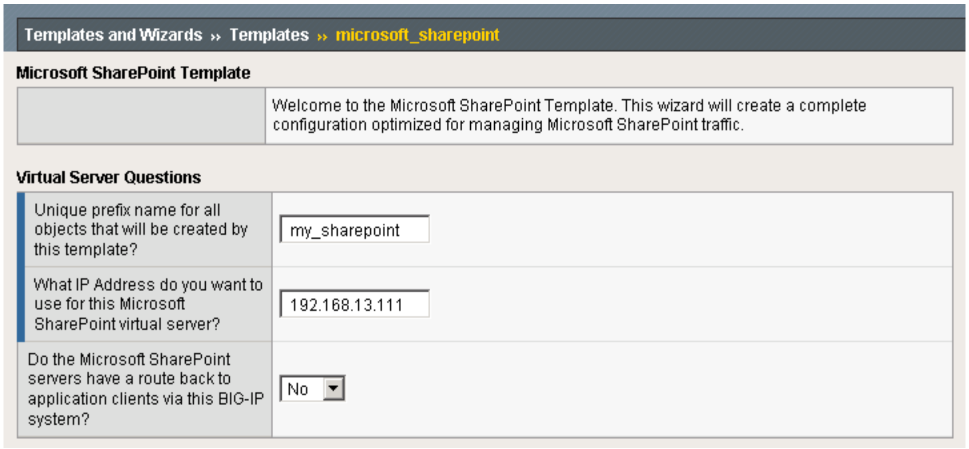
1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Microsoft SharePoint**. The SharePoint application template opens.
4. In the Virtual Server Questions section, complete the following:

   a) You can type a unique prefix for your SharePoint objects that the template will create. In our example, we leave this setting at the default, **my_sharepoint**.

   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 **192.168.13.111**.

   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**.



Templates and Wizards » Templates » microsoft_sharepoint

**Microsoft SharePoint Template**

| | |
|---|---|
| | Welcome to the Microsoft SharePoint Template. This wizard will create a complete configuration optimized for managing Microsoft SharePoint traffic. |

**Virtual Server Questions**

| | |
|---|---|
| Unique prefix name for all objects that will be created by this template? | my_sharepoint |
| What IP Address do you want to use for this Microsoft SharePoint virtual server? | 192.168.13.111 |
| Do the Microsoft SharePoint servers have a route back to application clients via this BIG-IP system? | No ▾ |

***Figure 1.3*** *Running the Microsoft SharePoint application template*

5. In the SSL Offload section, complete the following

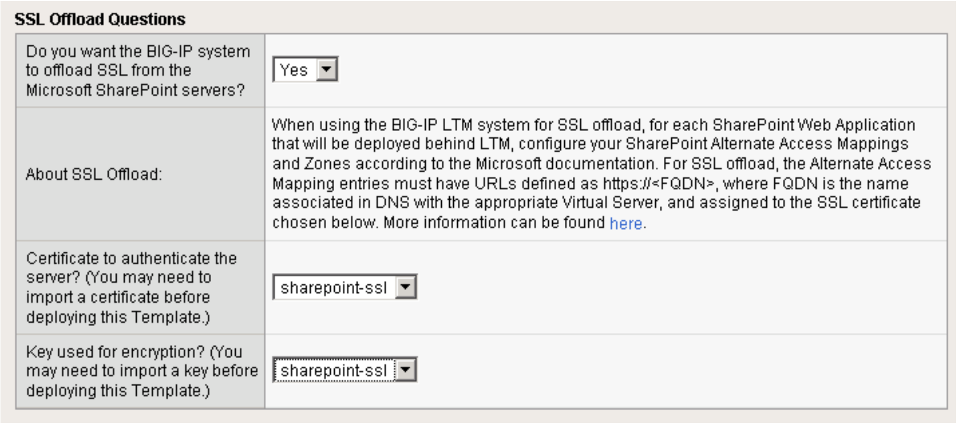
    a) if you are not using the BIG-IP system to offload SSL, leave this setting at the default, **No**. Continue with Step 6.

    If you are using the BIG-IP system to offload SSL from the SharePoint devices, select **Yes** from the list.
    The SSL options appear, including a note about configuring SharePoint Alternate Mappings and Zones (see the Configuration utility, or Figure 1.4 for the exact text). You can find more information at
    ***http://blogs.msdn.com/sharepoint/archive/2007/03/06/what-every-sharepoint-administrator-needs-to-know-about-alternate-access-mappings-part-1.aspx***

    b) 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 1-17.

    c) 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 1-17.

    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***.



**SSL Offload Questions**

| | |
|---|---|
| Do you want the BIG-IP system to offload SSL from the Microsoft SharePoint servers? | Yes |
| About SSL Offload: | When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, configure your SharePoint Alternate Access Mappings and Zones according to the Microsoft documentation. For SSL offload, the Alternate Access Mapping entries must have URLs defined as https://<FQDN>, where FQDN is the name associated in DNS with the appropriate Virtual Server, and assigned to the SSL certificate chosen below. More information can be found here. |
| Certificate to authenticate the server? (You may need to import a certificate before deploying this Template.) | sharepoint-ssl |
| Key used for encryption? (You may need to import a key before deploying this Template.) | sharepoint-ssl |

***Figure 1.4*** *Configuring the BIG-IP system for SSL Offload*

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 SharePoint devices that are a part of this deployment.
   In the **Address** box, type the IP address of the first SharePoint server. In our example, we type **10.132.82.101**.

   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 of the SharePoint devices.

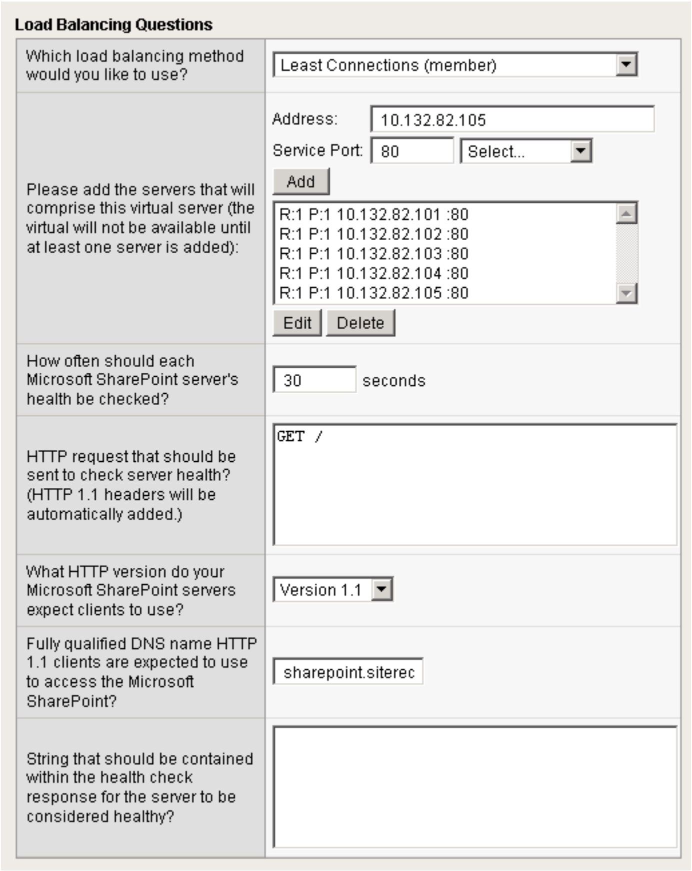
   c) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.

   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. Note that HTTP 1.1 headers are added to the GET by default.

   e) Select the HTTP version that the SharePoint 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 SharePoint. In the box, type the FQDN for your SharePoint deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **sharepoint.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: 10.132.82.105<br>Service Port: 80 Select...<br>R:1 P:1 10.132.82.101 :80<br>R:1 P:1 10.132.82.102 :80<br>R:1 P:1 10.132.82.103 :80<br>R:1 P:1 10.132.82.104 :80<br>R:1 P:1 10.132.82.105 :80 |
| How often should each Microsoft SharePoint 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 Microsoft SharePoint servers expect clients to use? | Version 1.1 |
| Fully qualified DNS name HTTP 1.1 clients are expected to use to access the Microsoft SharePoint? | sharepoint.siterec |
| String that should be contained within the health check response for the server to be considered healthy? | |

***Figure 1.5*** *Configuring the Load Balancing options*

7. In the Protocol and Security Questions section, complete the following

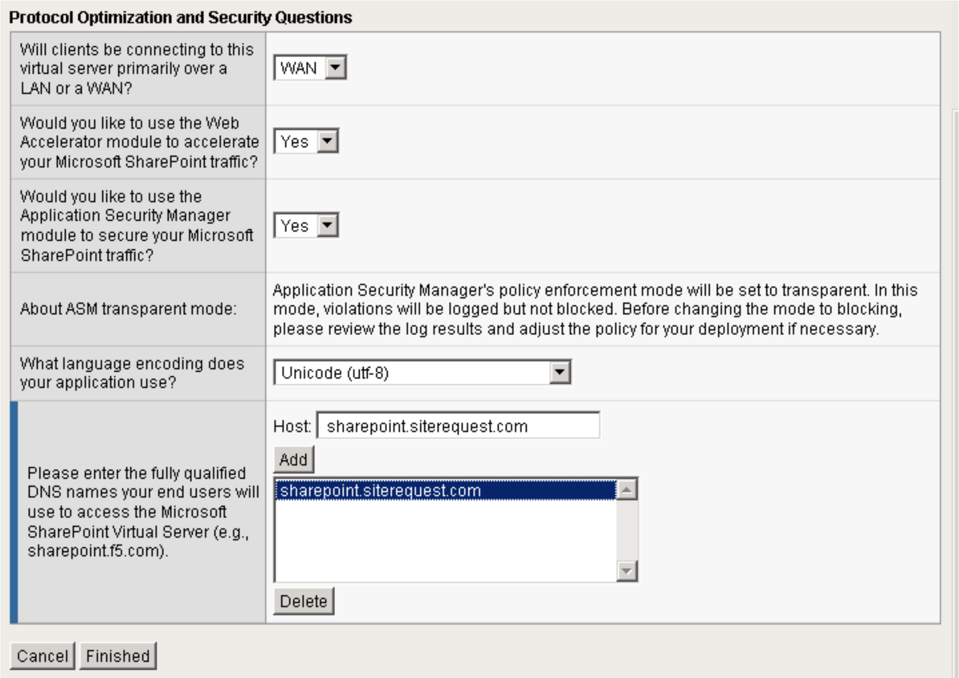
   a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list.
   This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.

   b) If you want to use the WebAccelerator module to accelerate the SharePoint 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 SharePoint deployments.

   c) If you want to use the Application Security Manager to secure the SharePoint 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 SharePoint 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 **sharepoint.siterequest.com** and click the **Add** button.



**Protocol Optimization and Security Questions**

| | |
|---|---|
| Will clients be connecting to this virtual server primarily over a LAN or a WAN? | WAN |
| Would you like to use the Web Accelerator module to accelerate your Microsoft SharePoint traffic? | Yes |
| Would you like to use the Application Security Manager module to secure your Microsoft SharePoint traffic? | Yes |
| 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? | Unicode (utf-8) |
| Please enter the fully qualified DNS names your end users will use to access the Microsoft SharePoint Virtual Server (e.g., sharepoint.f5.com). | Host: sharepoint.siterequest.com<br>Add<br>sharepoint.siterequest.com<br>Delete |

***Figure 1.6*** *Configuring the Protocol and Security options*

8. Click the **Finished** button.

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 SharePoint 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 SharePoint 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.

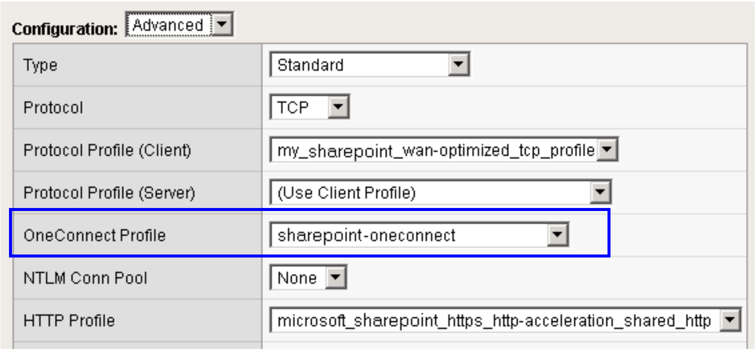
## To create a new OneConnect profile

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 Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sharepoint-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 SharePoint 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_sharepoint-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 **sharepoint-oneconnect**.
4. Click the **Update** button.



Configuration: Advanced

| | |
|---|---|
| Type | Standard |
| Protocol | TCP |
| Protocol Profile (Client) | my_sharepoint_wan-optimized_tcp_profile |
| Protocol Profile (Server) | (Use Client Profile) |
| OneConnect Profile | sharepoint-oneconnect |
| NTLM Conn Pool | None |
| HTTP Profile | microsoft_sharepoint_https_http-acceleration_shared_http |

***Figure 1.7*** *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_sharepoint_https_virtual_server**, and add our OneConnect profile.

This concludes the BIG-IP system configuration for Microsoft Office SharePoint 2007.

# 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. It is one of the following: **microsoft_sharepoint_http-wan-optimized-caching_shared_http microsoft_sharepoint_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.

## Deploying the Custom Logging role service

The next task is to deploy the Custom Logging role service. If you do not deploy this role service, you may receive a "Feature not supported" error when trying to edit the log definition in the next section.

### To deploy the Custom Logging role service

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open Server Manager.
2. In the Navigation pane, expand **Roles**.
3. Right-click **Web Server**, and then click **Add Role Services**.

4. Under *Health and Diagnostics*, check the box for **Custom Logging**, and then click the **Next** button.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** 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***

◆ **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***

### 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 in the Add Logging Field box, and then click the **OK** button in the Edit Logging Fields box.
6. Click a Log Definition to select it. By default, there is only one: %COMPUTERNAME%-Server. The log definition you select must have a status of Enabled.
7. From the Actions pane on the right, click **Edit Log Definition**.
8. Click the **Select Fields** button, and then check the box for the **X-Forwarded-For** logging field.
9. Click the **OK** button.
10. From the Actions pane, click **Apply**.

11. Click **Return To Advanced Logging**.
12. In the Actions pane, 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 SharePoint 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 v10 with Microsoft Office SharePoint 2007

- Creating the HTTP health monitor
- Creating the pool
- Creating profiles
- Creating the HTTP virtual server
- Creating a default SNAT
- Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL

# Manually configuring the BIG-IP LTM system with SharePoint 2007

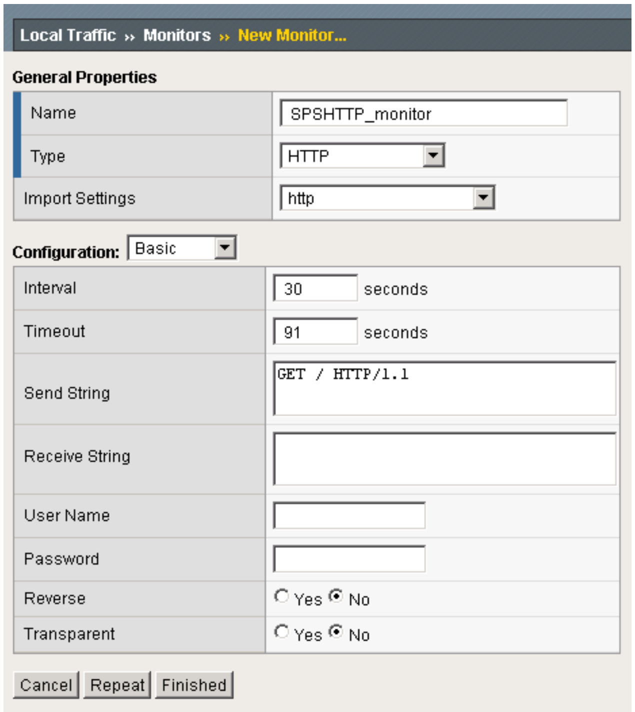
While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system rather than use the application template, perform the following procedures.

## Creating the HTTP health monitor

The first step is to set up health monitors for the SharePoint 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 configure a health monitor from the BIG-IP Configuration utility

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 **SPSHTTP_monitor**.
4. From the **Type** list, select **http**.
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.**
6. In the **Send String** box, type a string. In our example, we type **GET / HTTP/1.1** to request the default page at the root level. You can modify this string to request a different resource or otherwise modify it as appropriate for your environment; however, in all cases, the Send String must be a valid HTTP request.
7. In the **Receive String** box, you can type an optional Receive string.
8. Click the **Finished** button. The monitor is added to the Monitor list.



General Properties

| | |
|---|---|
| Name | SPSHTTP_monitor |
| Type | HTTP |
| Import Settings | http |

Configuration: Basic

| | |
|---|---|
| Interval | 30 seconds |
| Timeout | 91 seconds |
| Send String | GET / HTTP/1.1 |
| Receive String | |
| User Name | |
| Password | |
| Reverse | ○ Yes ● No |
| Transparent | ○ Yes ● No |

***Figure 2.1*** *Creating the HTTP Monitor*

# Creating the pool

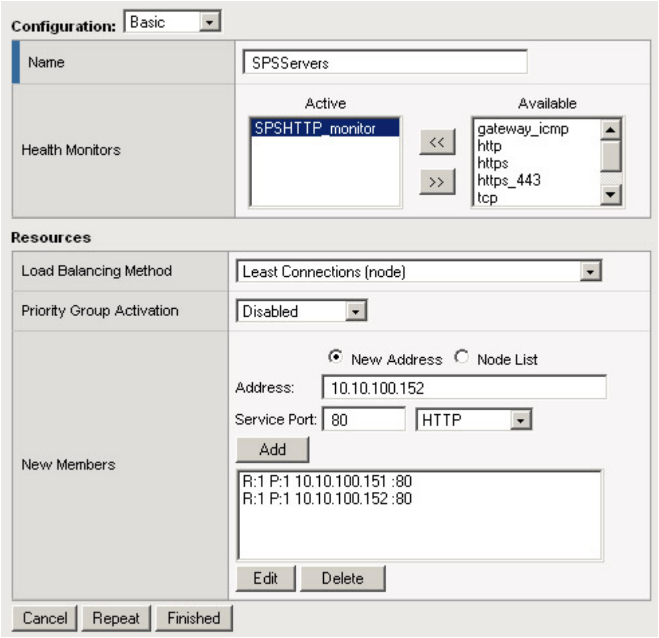
The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the SharePoint devices.

## To create the SharePoint 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 **SPSServers**.

4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (**<<**) button. In our example, we select **SPSHTTP_monitor**.
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 **10.10.100.151**.
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 9-11 for each server you want to add to the pool.
    In our example, we repeat these steps once for the remaining server, **10.10.100.152**.
12. Click the **Finished** button (see Figure 2.2).



Configuration: Basic

Name: SPSServers

Health Monitors
Active: SPSHTTP_monitor
Available: gateway_icmp, http, https, https_443, tcp

Resources

Load Balancing Method: Least Connections (node)

Priority Group Activation: Disabled

New Members
● New Address ○ Node List
Address: 10.10.100.152
Service Port: 80 HTTP

R:1 P:1 10.10.100.151 :80
R:1 P:1 10.10.100.152 :80

***Figure 2.2*** *Adding the SharePoint server pool*

# Creating profiles

BIG-IP version 9.0 and later use 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.

## Creating an HTTP profile

The first new profile we create is an HTTP profile. 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. There are a couple modifications to make no matter which profile you are using.
There are a couple of caveats for using this profile:

- If you are ***not*** terminating SSL (HTTPS) connections on the BIG-IP LTM, you must leave the **Redirect Rewrite** option at **None** (the default setting). **Redirect Rewrite** is meant to capture HTTP 3XX redirects and rewrite them to use HTTPS. See Step 5 in the following procedure.
- You must have Compression and RAM Cache licensed on your BIG-IP LTM system. Contact your Sales Representative for more information.

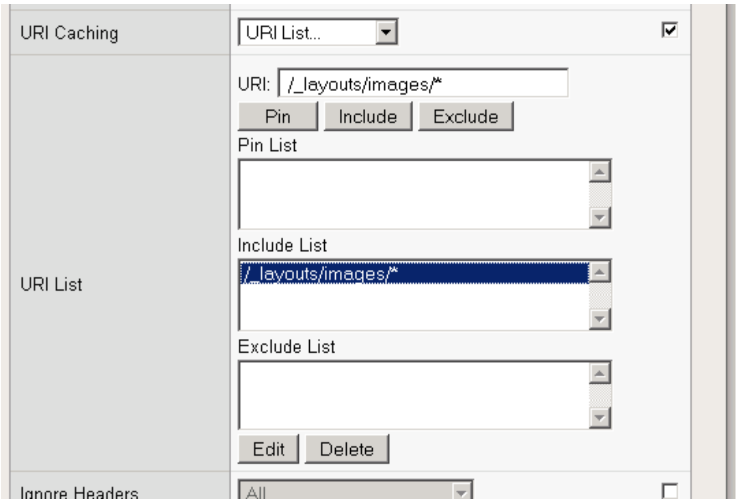
◆ **Note**

*The following procedure shows one way to optimize the Microsoft SharePoint 2007 configuration that has been tested in real-world scenarios by F5, and shown to give the greatest improvement. These procedures and the specific values given in some steps should be used as guidelines, modify them as applicable to your configuration.*

### 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. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **SPS_HTTP_opt**.
4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If not, select **http-wan-optimized-compression-caching**.

5. If you intend to terminate SSL (HTTPS) connections on the BIG-IP LTM, in the Settings section, check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Matching**. Otherwise, leave this at the default setting (**None**).
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 1-14 for detailed information, including modifications to IIS to accurately log the client IP address.
7. In the Compression section, check the Custom box for **Compression**, and from the **Compression** list, select **Enabled**.
8. In the RAM Cache section, check the Custom box for **URI Caching**, and leave **URI List** selected.
9. From the URI List section, in the **URI** box, type **/_layouts/images/*** and click the **Include** button. This ensures that all of the layout images are cached on the BIG-IP LTM system.



URI Caching: URI List... ☑

URI List:

URI: /_layouts/images/*

Pin List

Include List: /_layouts/images/*

Exclude List

Ignore Headers: All □

***Figure 2.3*** *Adding the image directory to the RAM cache URI include list.*

10. Modify any of the other settings as applicable for your network.
11. Click the **Finished** button.

## Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Microsoft SharePoint users are accessing the devices via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the 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 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 **SPS-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 **SPS-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 cookie persistence profile

The final profile we create is a Cookie Persistence profile. We recommend using the default cookie method for this profile (HTTP cookie insert), but you can change other settings, such as specifying a cookie expiration.

### 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 **SPSCookie**.
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.
7. Click the **Finished** button.

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

## 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 SharePoint 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 Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
   The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sharepoint-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.

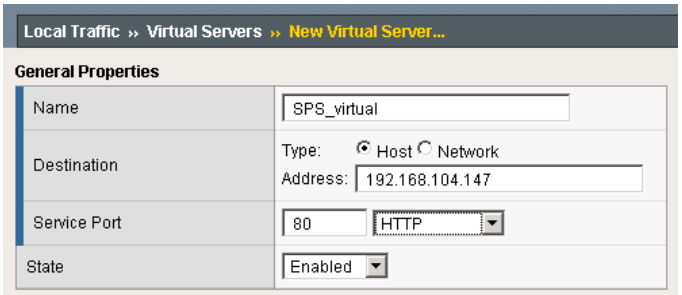
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

# Creating the HTTP virtual server

Next, we configure a HTTP virtual server that references the profiles and pool you created in the preceding procedures.

## To create the 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 **SPS_virtual**.
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 **192.168.104.147**.
6. In the **Service Port** box, type **80** or select **HTTP** from the list.



Local Traffic » Virtual Servers » New Virtual Server...

General Properties

| | |
|---|---|
| Name | SPS_virtual |
| Destination | Type: ● Host ○ Network<br>Address: 192.168.104.147 |
| Service Port | 80 HTTP |
| State | Enabled |

*Figure 2.4 Adding the SharePoint virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **SPS-tcp-wan**.

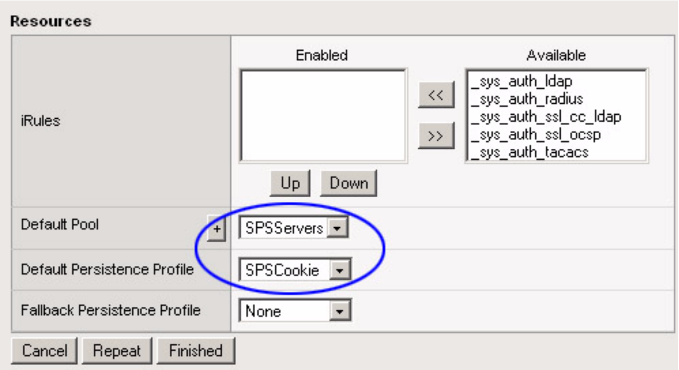
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **SPS-tcp-lan**.

11. From the **OneConnect Profile** list, select the profile you created in *Creating the OneConnect profile*. In our example, we select **sharepoint-oneconnect**.

12. From the **HTTP Profile** list, select the profile you created in the *Creating an HTTP profile* section. In our example, we select **SPSHTTP**.

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **SPSServers**.

14. 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 **SPSCookie**.



Resources

| | |
|---|---|
| Default Pool | SPSServers |
| Default Persistence Profile | SPSCookie |
| Fallback Persistence Profile | None |

***Figure 2.5*** *Resources section of the add virtual server page*

15. Click the **Finished** button.

# Creating a default SNAT

A secure network address translation (SNAT) ensures the proper routing of connections from the Index server to the Search server. In this configuration, we configure a default SNAT.

◆ **Note**

*If you do not want source address translation on client connections from the external VLAN, you can disable the default SNAT for the external VLAN.*

### To create a default SNAT

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
3. In the **Name** box, type a name for this SNAT. In our example, we type **DefaultSNAT**.
4. In the **Translation** list, select **Automap**.
5. ***Optional:*** If you to disable (or enable) the default SNAT for specific VLANs, from the VLAN Traffic list, select either **Enabled on** or **Disabled on** from the list. From the Available list, select the appropriate VLAN and click the Add (**<<**) button to move it to the Selected list.
6. Click the **Finished** button.

# Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL

This section describes how to configure the BIG-IP LTM system as an SSL proxy for a Microsoft Office SharePoint Server 2007 deployment. If you are not using the BIG-IP LTM system to offload SSL traffic, you do not need to perform these procedures.

◆ **Note**

*This section is written with the assumption that you have already configured your BIG-IP LTM system for a SharePoint deployment as described in this Deployment Guide.*

## Prerequisites and configuration notes

The following are additional prerequisites for this section:

- ◆ You need an SSL certificate for your site that is compatible with the BIG-IP LTM system. For more information, consult the BIG-IP documentation.
- ◆ You have already configured the BIG-IP LTM system as described in this Deployment Guide.
- ◆ ***Important:*** See *Configuring SharePoint Alternate Access Mappings to support SSL offload*, on page 1-3 for critical information about configuring SharePoint for the BIG-IP LTM and SSL offload.

This section contains following procedures for configuring the BIG-IP LTM system:

- *Using SSL certificates and keys*
- *Create a Client SSL profile*
- *Creating the Redirect iRule*
- *Modifying the HTTP virtual server*
- *Creating the HTTPS virtual server*

## Using SSL certificates and keys

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 SharePoint connections on the BIG-IP 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 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***.

## 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**.
   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.

# Create 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 based on the default 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 **SPS_clientssl**.
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.
9. Click the **Finished** button.

For more information on creating or modifying profiles, or SSL Certificates, see the BIG-IP documentation.

## Creating the Redirect iRule

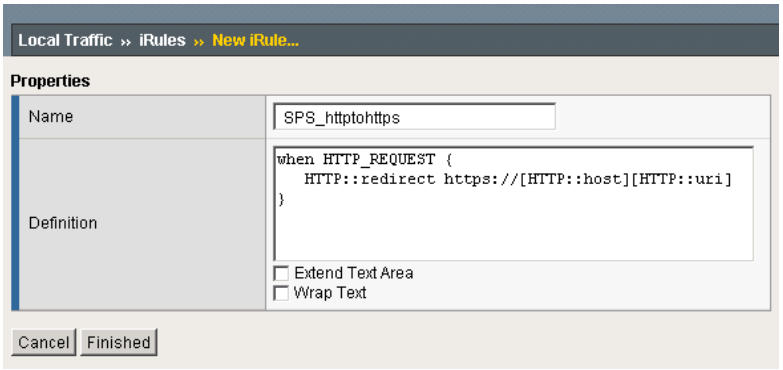
The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction

### 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 **SPS_httptohttps**.
4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {
   HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

5. Click the **Finished** button (see Figure 2.6).



Name: SPS_httptohttps

Definition:

```
when HTTP_REQUEST {
   HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

□ Extend Text Area
□ Wrap Text

***Figure 2.6*** *Creating the iRule*

# Modifying the HTTP virtual server

The next task is to modify the HTTP virtual server you created in *Creating the HTTP virtual server*, on page 8 to use the iRule you just created.

### To modify the existing SharePoint 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, click the SharePoint virtual server you created in the *Creating the HTTP virtual server* section. In our example, we click **SPS_virtual**.
3. On the menu bar, click **Resources**.
   The Resources page for the virtual server opens.
4. From the **Default Pool** list, select **None**. This virtual server no longer requires the load balancing pool, as traffic is redirected to the HTTPS virtual server we create in the following procedure.
5. Click the **Update** button.
6. In the iRules section, click the **Manage** button.
   The Resource Management screen opens.
7. From the **Available** list, select the iRule you created in the *Creating the Redirect iRule* section, and click the Add (<<) button. In our example, we select **SPS_httptohttps**.
8. Click the **Finished** button.

# Creating the HTTPS virtual server

The final task in this section is to create a HTTPS virtual server.

### To create a new 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 **SPS_httpsvirtual**.
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 **192.168.104.146**.
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. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **SPS-tcp-wan**.
10. 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 **SPS-tcp-lan**.
11. From the HTTP Profile list, select the name of the profile you created *Creating an HTTP profile* section. In our example, we select **SPS_HTTP_opt**.
12. From the **SSL Profile (Client)** list, select the name of the SSL profile you created in the *Create a Client SSL profile* section. In our example, we select **SPS_clientssl**.
13. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **SPSServers**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile*. In our example, we select **SPSCookie**.
15. Click the **Finished** button.

This concludes the BIG-IP LTM configuration.

# 3

# Deploying the WebAccelerator v10 with Microsoft Office SharePoint 2007

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

# Manually configuring the WebAccelerator module with SharePoint 2007

In this section, we configure the WebAccelerator module for SharePoint devices to increase performance for end users of SharePoint. 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 SharePoint devices as described in this Deployment Guide.
- You must have licensed and provisioned the WebAccelerator module on the BIG-IP LTM system.
- This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Microsoft Office SharePoint Server 2007. Consult the appropriate documentation for detailed information.
- If you are using BIG-IP LTM 9.4.2 or later, you should have configured an HTTP profile using the **http-acceleration** parent. See *Creating an HTTP profile*, on page 2-4 for more details.

## Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to Microsoft SharePoint servers. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency logs onto the SharePoint site via the WebAccelerator. The user’s request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so they can be served quickly without requiring the server to re-serve the same objects.

# Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. 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.

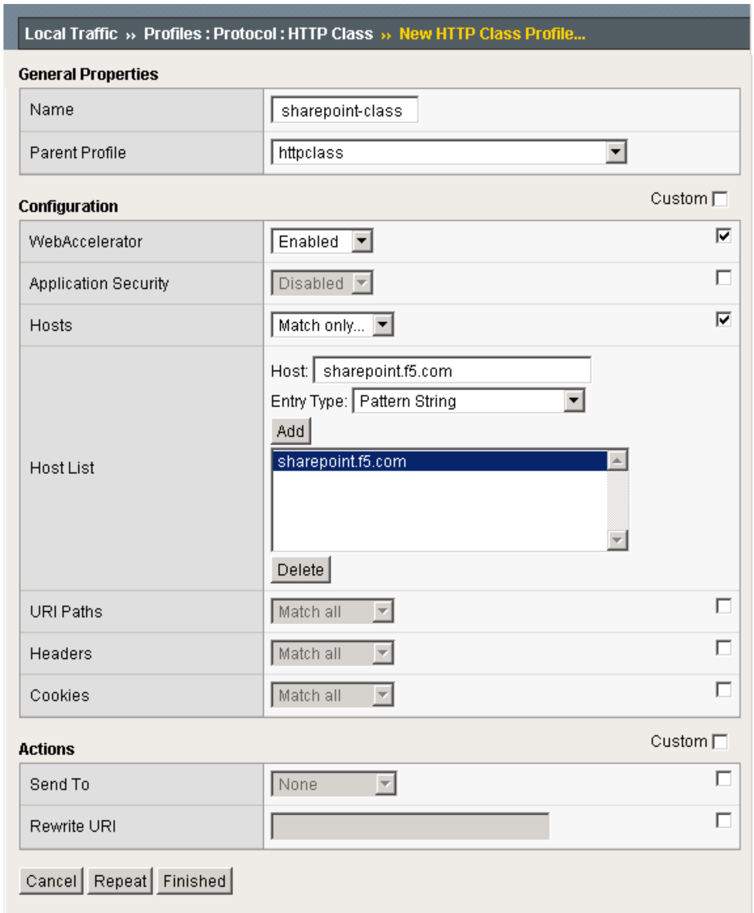
# Creating an HTTP Class profile

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 **sharepoint-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 the SharePoint site. In our example, we type **sharepoint.f5.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 the SharePoint deployment.
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.



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

**General Properties**

| | |
|---|---|
| Name | sharepoint-class |
| Parent Profile | httpclass |

**Configuration** Custom □

| | | |
|---|---|---|
| WebAccelerator | Enabled | ☑ |
| Application Security | Disabled | □ |
| Hosts | Match only... | ☑ |
| Host List | Host: sharepoint.f5.com<br>Entry Type: Pattern String<br>Add<br>sharepoint.f5.com<br>Delete | |
| URI Paths | Match all | □ |
| Headers | Match all | □ |
| Cookies | Match all | □ |

**Actions** Custom □

| | | |
|---|---|---|
| Send To | None | □ |
| Rewrite URI | | □ |

***Figure 3.1*** *Creating a new HTTP Class profile*

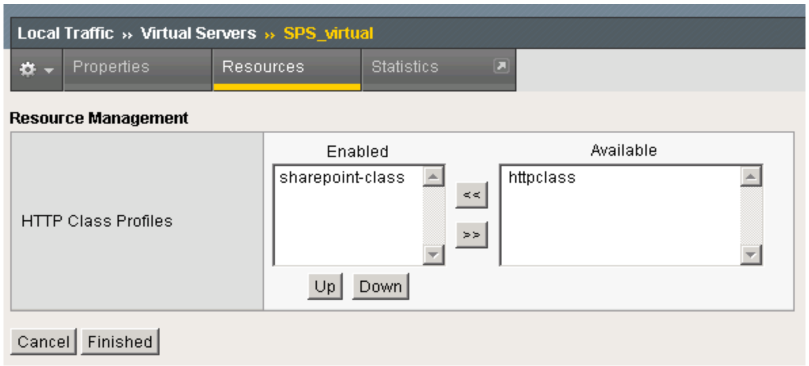
## Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your SharePoint deployment on the BIG-IP LTM system to use the HTTP Class profile you just created.

### 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 SharePoint deployment. In our example, we click **SPS_virtual**.
   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 **sharepoint_class** (see Figure 3.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.



HTTP Class Profiles

Enabled: sharepoint-class

Available: httpclass

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

# Creating an Application

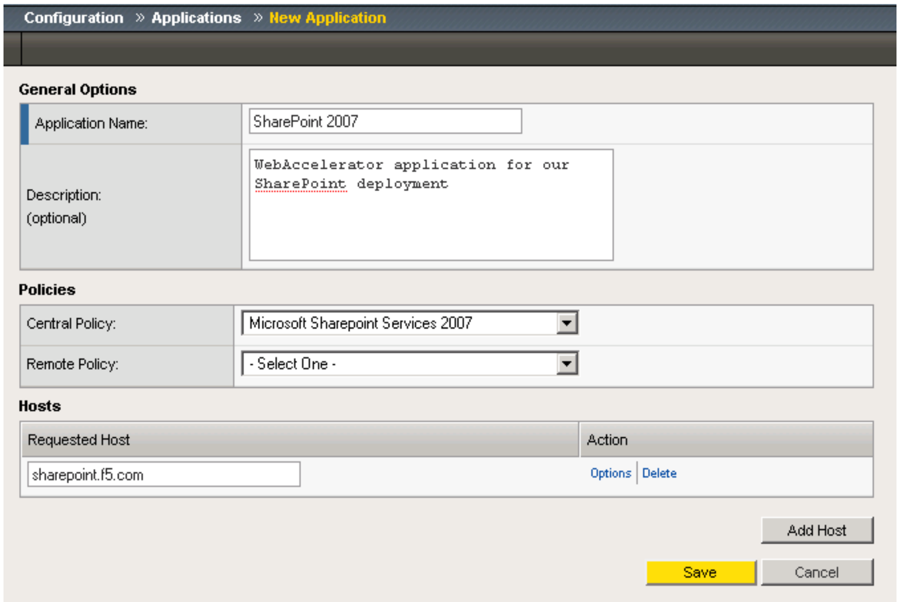
The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

## 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 **SharePoint 2007**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **Microsoft Sharepoint Services 2007**. This is a pre-defined policy created specifically for Microsoft Office SharePoint 2007 devices (see Figure 3.3).
6. In the **Requested Host** box, type the host name that your end users use to access the SharePoint site. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we

type **sharepoint.f5.com**
If you have additional host names, click the **Add Host** button and enter the host name(s).

7. Click the **Save** button.



Configuration » Applications » New Application

**General Options**

| | |
|---|---|
| Application Name: | SharePoint 2007 |
| Description:<br>(optional) | WebAccelerator application for our SharePoint deployment |

**Policies**

| | |
|---|---|
| Central Policy: | Microsoft Sharepoint Services 2007 |
| Remote Policy: | - Select One - |

**Hosts**

| Requested Host | Action |
|---|---|
| sharepoint.f5.com | Options \| Delete |

***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 an marked improvement in performance after their first visit.