

Deployment Guide

**Deploying Microsoft SharePoint
Portal Server 2003 with the F5
WebAccelerator**



Deploying Microsoft SharePoint with the F5 WebAccelerator

Welcome to the F5 WebAccelerator™ - Microsoft® SharePoint® Portal Server 2003 Deployment Guide. This guide provides detailed procedures on how to deploy the WebAccelerator with SharePoint devices to increase performance for end users of SharePoint. This configuration has been validated at a Microsoft Technology Center by F5.

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.

Microsoft SharePoint Portal Server 2003 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.

For more information on the Microsoft SharePoint Portal Server 2003, see <http://www.microsoft.com/office/sharepoint/prodinfo/default.mspx>

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

For more information on the BIG-IP system, see <http://www.f5.com/products/bigip/ltn/>.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ We assume that you have already configured the BIG-IP LTM system for directing traffic to the SharePoint devices. If you have not performed this configuration, see *Appendix A: Configuring the BIG-IP LTM system*, on page 7.
- ◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Microsoft SharePoint 2003. Consult the appropriate documentation for detailed information
- ◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later. If you are using a stand-alone WebAccelerator device, see *Appendix B: Configuring a stand-alone WebAccelerator device*, on page 13.

Configuration example

Using the configuration in this guide, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to Microsoft SharePoint servers. The WebAccelerator, and the BIG-IP LTM

with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content. Figure 1 shows a typical configuration.

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 that they can be served quickly without requiring the server to re-serve the same objects.

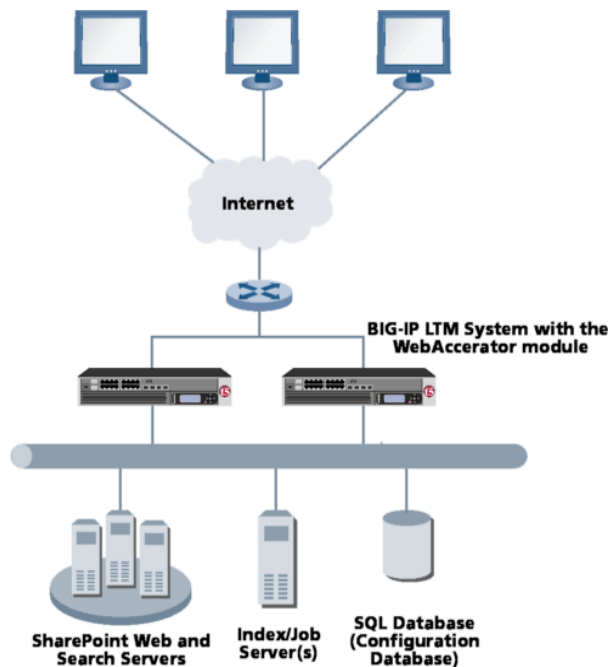


Figure 1 Configuration example

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.

If you have a stand-alone WebAccelerator device, and not the module, see *Appendix B: Configuring a stand-alone WebAccelerator device*, on page 13. If you have not configured the BIG-IP LTM system for directing traffic to the SharePoint devices, see *Appendix A: Configuring the BIG-IP LTM system*, on page 7.

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP LTM system's web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

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 **wa_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.company.com** (see Figure 2).
 - 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.

The screenshot shows the 'New HTTP Class Profile' configuration window. The breadcrumb trail is 'Local Traffic >> HTTP Class Profiles >> New HTTP Class Profile...'. The window is organized into three sections:

- General Properties:** Name: wa_class; Parent Profile: httpclass.
- Configuration:** Web Accelerator: Enabled; Hosts: Match only...; Host List: sharepoint.company.com; URI Paths: Match all; Headers: Match all; Cookies: Match all.
- Actions:** Send To: None; Rewrite URI: (empty field).

Buttons at the bottom include Cancel, Repeat, and Finished.

Figure 2 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 **sharepoint_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 **wa_class** (see Figure 3)
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

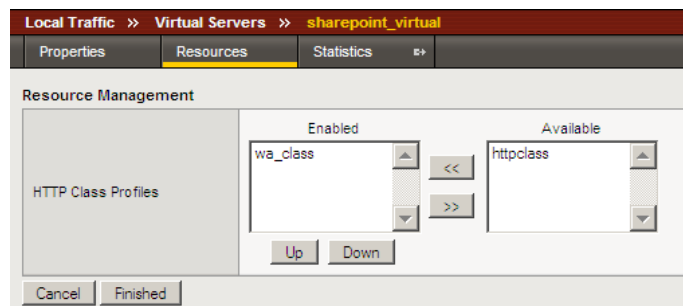


Figure 3 Adding the HTTP Class Profile to the Virtual Server

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**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **SharePoint**. This is a pre-defined policy created specifically for Microsoft SharePoint devices.
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.company.com**

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

7. Click the **Save** button.

The screenshot shows the 'New Application' configuration page in the F5 WebAccelerator. The breadcrumb navigation at the top reads 'Configuration » Applications » New Application'. The page is divided into three main sections: 'General Options', 'Policies', and 'Hosts'.
 - **General Options:** Contains a text box for 'Application Name' with the value 'SharePoint', and a larger text area for 'Description (optional)' containing the text 'This application points to our internal sharepoint deployment.'
 - **Policies:** Features a dropdown menu for 'Local Policies' currently set to 'SharePoint'.
 - **Hosts:** A table with two columns: 'Requested Host' and 'Action'. The first row has 'sharepoint.company.com' in the first column and 'Options | Delete' in the second. Below the table is an 'Add Host' button.
 At the bottom right of the form are two buttons: 'Save' (highlighted in yellow) and 'Cancel'.

Figure 4 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.

Appendix A: Configuring the BIG-IP LTM system

If you do not already have the BIG-IP LTM system configured for directing traffic to the SharePoint devices, you need to use the following procedures to create a health monitor, pool, profiles, and a virtual server. If you already have an existing BIG-IP/SharePoint deployment, it is highly likely you already have these items configured on your BIG-IP LTM system; in this case, continue to *Configuring the WebAccelerator module*, on page 2.

To configure the base BIG-IP LTM system, you must complete the following procedures:

- *Connecting to the BIG-IP device*
- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating Profiles*
- *Creating the virtual server*

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Creating the HTTP health monitor

The next step is to set up a health monitor for the web servers (nodes). This procedure is optional, but very strongly recommended. In our example, 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. We configure the health monitors first in version 9.0 and later, as health monitors are now associated at the pool level.

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 **SPSHTTP_monitor**.
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 (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. **Optional:** In the **Send String** and **Receive Rule** sections, you can add an optional Send String and Receive Rule specific to the device being checked.

The screenshot displays the 'New Monitor...' configuration window. The breadcrumb trail at the top reads 'Local Traffic >> Monitors >> New Monitor...'. The 'General Properties' section includes a 'Name' field with 'SPSHTTP_monitor', a 'Type' dropdown menu set to 'HTTP', and an 'Import Settings' dropdown set to 'http'. Below this, the 'Configuration' section is set to 'Basic'. It features two input fields: 'Interval' with the value '30' and 'seconds', and 'Timeout' with the value '91' and 'seconds'. The 'Send String' field contains the text 'GET / HTTP/1.0'. The 'Receive String' field is currently empty.

Figure 5 Creating the HTTP monitor

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

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 **Predictive**.
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 6).

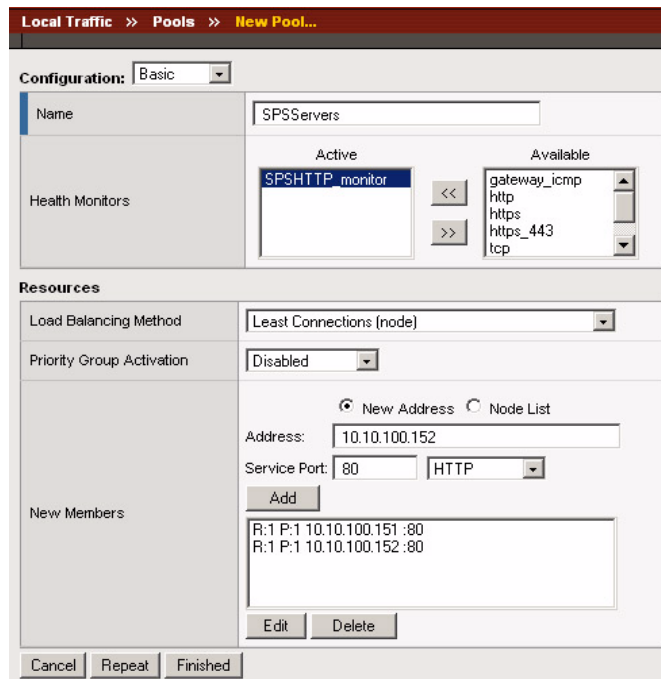


Figure 6 Adding the SharePoint server pool

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.

For this configuration, we create two new profiles: an HTTP profile and a cookie persistence profile.

◆ Tip

For additional information about configuring the BIG-IP LTM system for SharePoint devices, including using Profiles to optimize the configuration, see the BIG-IP - SharePoint Deployment Guide:

http://www.f5.com/solutions/deployment/pdfs/sharepoint_bigip9_dg.pdf

Creating an HTTP profile

The first new profile we create is an HTTP profile. 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 HTTP profile based on the default HTTP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP 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 **SPSHTTP**.
5. From the **Parent Profile** list, ensure that **HTTP** is selected.
6. Modify any of the other 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 a cookie persistence profile

The next 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 based on the default 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 virtual server

The next task is to create a virtual server that references the pool. For the purposes of the Deployment Guide, we configure an HTTP virtual server.

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 **sharepoint_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 **172.27.90.110**.
6. In the **Service Port** box, type **80**.
7. Modify the options in the Configuration section as applicable for your deployment.
8. In the Resources section, from the **Default Pool** list, select the name of the pool you created in the *Creating the pool* section. In our example we select **SPSServers**.
9. Modify the other options in the Resources section as applicable for your configuration.
10. Click the **Finished** button.

Appendix B: Configuring a stand-alone WebAccelerator device

Use this section if you have a WebAccelerator device, and not the module on the BIG-IP LTM system. Configuring a stand-alone device is quite simple, and only requires you create a WebAccelerator 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.

Connecting to the WebAccelerator device

Use the following procedure to access the WebAccelerator system's web-based Configuration utility using a web browser.

To connect to the WebAccelerator using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the device:8443>
2. Type your user name and password, and click **OK**.
The Home screen opens.

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**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **SharePoint**. This is a pre-defined policy created specifically for Microsoft SharePoint devices.

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.company.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:

Description: (optional)

Policies

Local Policies:

Hosts

Requested Host	Action
<input type="text" value="sharepoint.company.com"/>	Options Delete

Figure 7 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.