



What's inside:

- 2 What is F5 iApp™?
- 2 Prerequisites and configuration notes
- 3 Configuration example
- 4 Preparation Worksheet
- 5 Configuring the BIG-IP iApp for Microsoft SharePoint 2010
- 10 Next steps
- 12 Configuring BIG-IP Access Policy Manager for SharePoint 2010
- 15 Appendix: Manual configuration table
- 18 Appendix B: Configuring DNS and NTP on the BIG-IP system
- 19 Document Revision History

Deploying the BIG-IP System v11 with Microsoft SharePoint 2010

Welcome to the F5 and Microsoft® SharePoint® 2010 Deployment Guide. This document contains guidance on configuring the BIG-IP system version 11 for SharePoint 2010, resulting in a secure, fast, and available deployment.

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy, accurate way to configure the BIG-IP system for Microsoft SharePoint 2010.

SharePoint Server 2010 enables innovative business collaboration for organizations around the world. F5 has developed a flexible and intelligent application delivery network for SharePoint 2010 that drives your business ahead.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: <http://devcentral.f5.com/Microsoft/>.

Why F5?

F5 offers a complete suite of application delivery technologies designed to provide a highly scalable, secure, and responsive SharePoint deployment. In addition, the F5 solution for SharePoint Server includes management and monitoring features to support a cloud computing infrastructure.

- The BIG-IP system can reduce the burden on servers by monitoring SharePoint Server responsiveness across multiple ports and protocols, driving intelligent load balancing decisions.
- CPU-intensive operations such as compression, caching, and SSL encryption/decryption can be offloaded onto the BIG-IP system, which can extend SharePoint Server capacity by 25%
- F5 WAN optimization technology can dramatically increase SharePoint 2010 performance
- F5 enables organizations to achieve dramatic bandwidth reduction for remote office SharePoint users.
- F5 protects SharePoint deployments that help run your business with powerful application-level protection, as well as network- and protocol-level security.
- The BIG-IP Access Policy Manager, F5's high-performance access and security solution, can provide proxy authentication and secure remote access to Microsoft SharePoint 2010.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Products and versions tested

Product	Versions
BIG-IP system	11.0, 11.0.1, 11.1
Microsoft SharePoint Server	2010

Important: Make sure you are using the most recent version of this deployment guide, available at <http://www.f5.com/pdf/deployment-guides/sharepoint-2010-iapp-dg.pdf>.

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for Microsoft SharePoint acts as the single-point interface for building, managing, and monitoring SharePoint 2010.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network*: <http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf>.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- For this deployment guide, the BIG-IP system **must** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.

This deployment guide provides guidance for using the iApp for Microsoft SharePoint 2010 found in version 11.0 and later. While we recommend using the iApp template, for users familiar with the BIG-IP system there is a manual configuration table at the end of this guide that describes how to configure the individual objects.

- This document is written with the assumption that you are familiar with both F5 devices and Microsoft SharePoint. For more information on configuring these devices, consult the appropriate documentation.
- If you have licensed and provisioned the BIG-IP Access Policy Manager and want to use it for SharePoint 2010, see *Configuring BIG-IP Access Policy Manager for SharePoint 2010* on page 15 after completing the iApp. You must manually configure APM.

For BIG-IP APM, you must have configured NTP and DNS on the BIG-IP system. See *Appendix B: Configuring DNS and NTP on the BIG-IP system* on page 23 for configuration information.

- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system.
- 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

Important



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 5*.

Note



- If you require the BIG-IP system to re-encrypt SSL traffic before sending it to the SharePoint devices (SSL Bridging), there are additional procedures to perform after running the iApp. See *Optional: Configuring SSL Bridging on the BIG-IP LTM on page 18*. If your SharePoint web application uses Basic authentication, we recommend SSL Bridging, as user passwords are sent in clear text between the BIG-IP system and SharePoint servers.
- This deployment guide contains guidance on optional modules, including Application Visibility Reporting, WebAccelerator, Application Security Manager (ASM), and Access Policy Manager (APM). To take advantage of these modules, they must be fully licensed and provisioned before starting the iApp template. For more information on licensing modules, contact your sales representative. Note that AVR is licensed on all systems, but must be provisioned before beginning the iApp template.

Tip



- If you are using Microsoft FAST Search Server 2010 for SharePoint 2010, see <http://www.f5.com/pdf/deployment-guides/microsoft-fast-search-2010-dg.pdf>

Configuration example

The following traffic flow diagram shows the configuration described in this deployment guide.

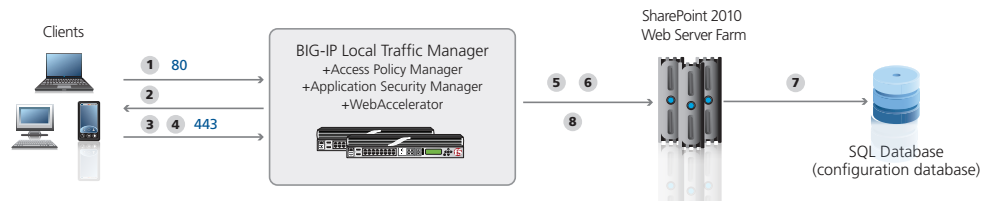


Figure 1: Logical configuration example

The traffic flow for this deployment guide configuration is as follows:

1. The client makes a connection to the BIG-IP virtual server IP address for the SharePoint 2010 devices.
2. Depending on the configuration, the BIG-IP system may use an iRule to redirect the client to an encrypted (HTTPS) form of the resource.
3. If you are using BIG-IP APM, the APM authenticates the user according to the Access policy.
4. The client machine makes a new connection to the BIG-IP virtual server IP address of the SharePoint server to access the resource over an encrypted connection.
5. The next step depends on whether you are using ASM, WebAccelerator or both:
 - If you are using the BIG-IP ASM, the ASM inspects the connection to check for possible security violations. If there are no violations, the connection continues.
 - If you are using the BIG-IP WebAccelerator, the WebAccelerator uses caching and other techniques to speed the connection.
6. The BIG-IP LTM chooses the best available SharePoint device based on the load balancing algorithm and health monitoring.
7. The SharePoint application interacts with the SQL (configuration) database.
8. The BIG-IP LTM uses persistence to ensure the clients persist to the same server, if applicable.

Preparation Worksheet

In order to use the iApp for SharePoint 2010, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➤ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	SSL Offload	Pool Members	Sync/Failover Groups*	TCP request queuing*	WAN or LAN clients
<p>IP address you will use for the LTM virtual server:</p> <p>FQDN that will resolve to the virtual server address:</p>	<p><i>Offloading SSL?</i> Yes No</p> <p>If offloading SSL, import a certificate and key into the BIG-IP LTM before running the template.</p> <p>Certificate:</p> <p>Key:</p> <p><i>Be sure to see Configuring SharePoint Alternate Access Mappings to support SSL offload on page 5.</i></p> <p><i>Also see Optional: Configuring SSL Bridging on the BIG-IP LTM on page 18</i></p>	<p>SharePoint server IP addresses:</p> <p>1:</p> <p>2:</p> <p>3:</p> <p>4:</p> <p>5:</p> <p>6:</p> <p>7:</p> <p>8:</p> <p>9:</p> <p>10:</p> <p>Port used by SharePoint:</p>	<p>If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group</p> <p>Device Group name:</p> <p>Traffic Group name:</p>	<p>If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node.</p> <p>Request queue length:</p> <p>Timeout:</p> <p>Node Connection limit:</p>	<p>Most clients connecting through BIG-IP to SharePoint are coming over a:</p> <p>LAN</p> <p>WAN</p>
Optional Modules (you must have provisioned modules before running the template)					
<i>Access Policy Manager (APM)**</i>		<i>WebAccelerator*</i>	<i>Application Visibility Reporting (AVR)*</i>		<i>Application Security Manager (ASM)*</i>
<p>Name or IP address of an Active Directory Server in your Domain that the BIG-IP can contact:</p> <p>What is the Active Directory Domain name for SharePoint users?</p> <p>If your Active Directory domain does not allow anonymous binding, you need a user account with administrative permissions.</p> <p>Username:</p> <p>Password:</p>		<p>All FQDNs for SharePoint:</p> <p>1:</p> <p>2:</p> <p>3:</p> <p>4:</p> <p>5:</p>	<p>If using AVR, we strongly recommend you first create a custom Analytics profile before running the template.</p> <p>Analytics profile name:</p>		<p>Language encoding the application uses (the default is Unicode (utf-8)):</p>

* *Optional*

** *BIG-IP APM is not a part of the iApp and must be configured manually*

Configuring SharePoint Alternate Access Mappings to support SSL offload

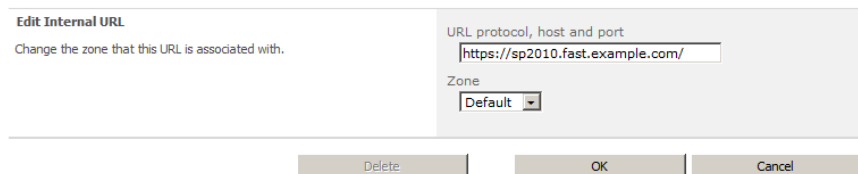
When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the BIG-IP LTM SSL virtual server and ensure correct rewriting of 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.

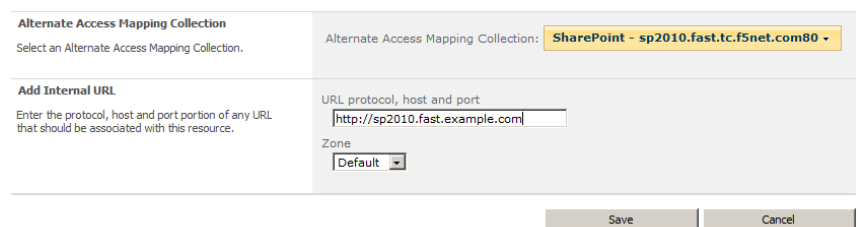
For more information, see <http://sharepoint.microsoft.com/blog/Pages/BlogPost.aspx?piD=804>.

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.

- From the navigation pane, click **Application Management**, and then under **Service Applications**, click **Manage service applications**.
- 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.
- In the navigation pane, click **Content Sources**.
- On the Menu bar, click **New Content Source**.
- In the **Name** box, type a name. We type **https://sp2010.fast.example.com**.
- In the Start Addresses section, type the appropriate HTTPS URL. In our example, we type **https://sp2010.fast.example.com**. All other settings are optional.
- Click the **OK** button.
- Repeat this entire procedure for each public URL to be deployed behind LTM.

The screenshot shows the 'FAST Content SSA: Add Content Source' page in SharePoint 2010 Central Administration. The page has a navigation pane on the left with sections for Administration, Crawling, and Reports. The main content area is titled 'Use this page to add a content source.' and contains several sections: 'Name' (with a text box containing 'https://sp2010.fast.example.com'), 'Content Source Type' (with radio buttons for 'SharePoint Sites', 'Web Sites', 'File Shares', 'Exchange Public Folders', 'Line of Business Data', and 'Custom Repository', where 'SharePoint Sites' is selected), 'Start Addresses' (with a text area containing 'https://sp2010.fast.example.com' and an example of 'http://intranetsite'), and 'Crawling Settings' (with a section for selecting crawling behavior).

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

After configuring Alternate Access Mappings in SharePoint 2010 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

- From SharePoint Central Administration navigation pane, click **Application Management**.
- Under Service Applications, click **Manage service applications**.
- 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).
- From the navigation pane, under Crawling, click **Index Reset**.

5. Click the **Reset Now** button to reset all crawled content.

Reset all crawled content
Resetting the crawled content will erase the content index. After a reset, search results will not be available until crawls have been run.

Warning:
You need to manually clear the content collection on the backend after you have reset all crawled content in this service application, and before starting any new crawls.
The content index has already been fed into a content collection on the FAST Search for SharePoint backend. You must clear the content from this specific content collection on the backend to ensure data remains in sync. To do this, use PowerShell commandlets. Load the Microsoft.FASTSearch.PowerShell snapin and use the command Clear-FASTSearchContentCollection. Note that this is irreversible. Ensure that you clear the same collection as used by this service application.

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.

Select what the priority of this content source should be. The Crawl system will prioritize the processing of 'High' priority content sources over 'Normal' priority content sources

Priority | normal ▾

Start Full Crawl
Select "Start full crawl of this content source" and click "OK" to start a full crawl of this content source.

Start full crawl of this content source

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

Configuring the BIG-IP iApp for Microsoft SharePoint 2010

Use the following guidance to help you configure the BIG-IP system for Microsoft SharePoint 2010 using the BIG-IP iApp template.

Getting started with the iApp for SharePoint 2010

To begin the SharePoint iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **SharePoint-2010_**.
5. From the **Template** list, select **f5.microsoft_sharepoint_2010**.
The Microsoft SharePoint 2010 template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**

If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

a. **Device Group**

If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

b. **Traffic Group**

If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Analytics

This section of the template asks questions about Analytics. The Application Visibility Reporting (AVR) module allows you to view statistics specific to your Microsoft SharePoint 2010 implementation. AVR is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that these are only for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile before beginning the template. To create a new profile, from the Main tab, select Profiles and then click Analytics. Click New and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions.

1. **Enable Analytics**

Choose whether you want to enable AVR for Analytics.

2. **Analytics Profile**

You must decide whether to use the default Analytics profile, or create a new one. As

Tip

If using AVR, create a new Analytics profile before beginning the iApp for more specific reporting

mentioned previously, we recommend creating a new profile to get the most flexibility and functionality out of AVR. If you choose to create a new profile after starting the template, you must exit the template, create the profile, and then restart the template.

To use the default Analytics profile, choose Use **Default Profile** from the list.

To choose a custom profile, leave the list set to **Select a Custom Profile**, and then from the Analytics profile list, select the custom profile you created.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**

This is the address clients use to access SharePoint 2010 (or a FQDN will resolve to this address). You need an available IP address to use here.

2. **Port for the virtual server**

This is the applicable service port. If you are using the BIG-IP LTM to offload SSL, we recommend using 443. The default is 80.

3. **Routes or secure network address translation**

If the SharePoint servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #4) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new source address as the destination address when responding to traffic originating through the BIG-IP.

If you indicate the SharePoint servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the SharePoint servers.

We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

If you are configuring your BIG-IP LTM in a "one-armed" configuration with your SharePoint servers -- where the BIG-IP virtual server(s) and the SharePoint servers have IP addresses on the same subnet -- you must choose No.

4. **More than 8,000 simultaneous users**

If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #5.

If you have a very large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**.

Repeat for any additional IP addresses.

5. **NTLM**

If you have configured the SharePoint servers to use NTLM authentication, select Yes from the list. If the SharePoint servers do not use NTLM, leave the list set to No.

SSL Encryption questions

Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the **Configuration Guide for BIG-IP Local Traffic Manager** available at <http://support.f5.com/kb/en-us.html>.

1. **Offload SSL?**

If you want the BIG-IP system to offload SSL processing from the SharePoint Servers (recommended), select **Yes** from the list, and answer the following two questions. If you do not want to offload SSL, select **No**, and then continue with the next section.

- a. **Certificate**

Select the certificate for you imported for SharePoint from the certificate list.

- b. **Key**

Select the associated key from the list.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the SharePoint servers, and configure the health monitor and pool.

1. **New Pool**

Choose **Create New Pool**, unless you have already made a pool on the LTM for the SharePoint devices. If you have already created a pool, select it from the list.

2. **Load balancing method**

While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

3. **Address/Port**

Type the IP Address and Port for each SharePoint server. You can optionally add a Connection Limit (see note on the left). Click **Add** to add additional servers to the pool.

4. **TCP Request Queuing**

TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *New Features Guide for BIG-IP Version 11*, available on Ask F5.

Important →

TCP Request Queuing is an advanced feature and should be used with caution.

If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port for the SharePoint Server nodes.

If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.

- a. Type a queue length in the box. Leaving the default of 0 is not recommended.

- b. Type a number of milliseconds for the timeout value.

5. **Health Monitor**

Choose **Create New Monitor**, unless you have already made a health monitor on the LTM for the SharePoint devices. If you have created a SharePoint monitor, select it from the list.

6. **Interval**
Specifies how often the system checks the health of the servers. We recommend the default of 30 seconds.
7. **HTTP Request**
This is optional. You can configure the template to retrieve a specific page by typing the path here. Leaving the default (GET /) marks the node up if anything is returned from the web page.
8. **HTTP version**
Unless the majority of your users are using HTTP 1.0 (not common), we recommend selecting **Version 1.1** from the list.
 - **FQDN:** When you select Version 1.1, a new row appears asking for the FQDN the clients use to access SharePoint. Type it here.
9. **Monitor response string**
Optional. If you configured a unique HTTP Request, type the expected response.

Protocol Optimization and Security Questions

In this section, you configure security and protocol optimizations.

1. **WAN or LAN**
Specify whether most clients are connecting over a WAN or LAN. Because most SharePoint clients are likely to be coming over the WAN, we recommend selecting WAN (the default).
2. **WebAccelerator**
If you have licensed and provisioned the WebAccelerator module, you have the option of using it for SharePoint 2010. The WebAccelerator provides application acceleration for remote users. As noted above, do not deploy WebAccelerator if you plan on using Application Security Manager.
 - a. *DNS names*
If you select Yes, an additional row appears in the template asking for the fully qualified domain names used for SharePoint 2010. The BIG-IP system uses these entries for the Requested Hosts field, allowing the WebAccelerator module to accelerate the traffic to these virtual hosts.

In the **Host** box, type the **FQDN**. If you have additional FQDNs, click the **Add** button.
 - b. *X-WA-info Header*
By default, the WebAccelerator X-WA-info header is not included in the response from the BIG-IP. This header is useful for debugging WebAccelerator behavior. There are two additional options:
 - Standard: If you choose Standard, the BIG-IP inserts a HTTP header that includes numeric codes which indicate if and how each object was cached.
 - Debug: If you choose Debug, the BIG-IP includes extended information which may help for extended troubleshooting.
 - c. *WebAccelerator Performance monitor*
While the BIG-IP Dashboard provides statistics and performance graphs related to WebAccelerator, you can choose to enable the WebAccelerator performance monitor for legacy WebAccelerator performance monitoring for debugging purposes. The results can be found in the Main tab of the navigation page, under WebAccelerator, by clicking Traffic Reports.

In our example, we leave the performance monitor **Disabled**.

Important



Enabling performance monitoring for a WebAccelerator application can degrade overall performance and should only be used temporarily. If you choose to deploy the monitor at this time, we recommend you re-enter the iApp after collecting relevant data, and disable the monitor.

d. *WebAccelerator policy*

For this template, F5 recommends the **Microsoft SharePoint 2010** policy to achieve the best results for Web acceleration of SharePoint traffic. Should F5 publish an updated policy to DevCentral that you have downloaded and imported, or if a custom policy is created for your environment (locally), you can select that custom policy from the list. In our example, we leave the default, **Microsoft SharePoint 2010**.

3. **Application Security Manager**

If you have licensed and provisioned the Application Security Manager (ASM), you have the option of using it to protect SharePoint 2010. The ASM module is an advanced web application firewall that significantly reduces and mitigates the risk of loss or damage to data, intellectual property, and web applications.

As noted on the previous page, do not deploy ASM if you plan on using WebAccelerator.

Important



If you choose to use ASM, the iApp template sets the policy enforcement mode to transparent. In this mode, violations are logged but not blocked. Before changing the mode to blocking, review the log results and adjust the policy for your deployment if necessary.

- a. If you select **Yes**, an additional row appears asking for the language encoding. Select the proper language from the list.

Finished

Review your answers to the questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the SharePoint 2010 service you just created. To see the list of all the configuration objects created to support SharePoint 2010, on the Menu bar, click **Components**. The complete list of all SharePoint related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Note



If you have licensed and provisioned the BIG-IP Access Policy Manager and want to use it for SharePoint 2010, see *Configuring BIG-IP Access Policy Manager for SharePoint 2010* on page 15.

If you require the BIG-IP LTM to re-encrypt traffic before sending it to the SharePoint servers, see *Optional: Configuring SSL Bridging on the BIG-IP LTM* on page 18.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the SharePoint 2010 implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your SharePoint Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the SharePoint configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. And you can always get object-level statistics.

AVR statistics

If you have provisioned AVR, you can get application-level statistics for your SharePoint application service.

To view AVR statistics

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the Application Service List, click the SharePoint 2010 service you just created.
3. On the Menu bar, click **Analytics**.

4. Use the tabs and the Menu bar to view different statistics for your SharePoint 2010 iApp.

Object-level statistics

If you haven't provisioned AVR, or want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Configuring BIG-IP Access Policy Manager for SharePoint 2010

In this section, we provide guidance on manual configuring the BIG-IP Access Policy Manager (APM) for use with SharePoint 2010. The BIG-IP APM, F5's high-performance access and security solution, can provide proxy authentication and secure remote access to Microsoft SharePoint 2010. A future version of the iApp template will include BIG-IP APM.

To add APM to the SharePoint iApp configuration, you must first configure the BIG-IP APM manually using the table on this page. After configuring the BIG-IP APM, you must disable Strict Updates on the iApp Application Service in order to attach the Access Profile to the virtual server created by the template.

Using the configuration table

Use the following table to manually configure the BIG-IP APM for SharePoint. This table contains a list of BIG-IP configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP APM Object	Non-default settings/Notes	
DNS and NTP	See <i>Appendix B: Configuring DNS and NTP on the BIG-IP system on page 23</i> for instructions.	
AAA Servers (Access Policy -->AAA Servers)	Name Type Domain Controller Domain Name Admin Name/Password	Type a unique name Active Directory Type the IP address of the Domain controller Type the Windows Domain FQDN If required, type the Admin name and Password
SSO Configurations (Access Policy--> SSO Configurations)	Name SSO Method NTLM Domain	Type a unique name. NTLMV1 Type the NTLM Domain name
Access Profile (Access Policy -->Access Profiles)	Name Restrict to Single Client IP* Cookie Options Languages	Type a unique name. Enable this feature for additional security when using the Persistent cookie setting Click a check in the Persistent Cookie box Move the appropriate language(s) to the Accepted box.
Access Policy	Edit	Edit the Access Profile you created using the Visual Policy Editor. See the procedure on this page.

* Optional. Checking this box restricts each APM session to a single source IP address. When a client's source IP address changes, it will be required to reauthenticate to APM. Because persistent cookies are more easily compromised than browser session cookies, F5 recommends enabling this setting when using persistent APM cookies.

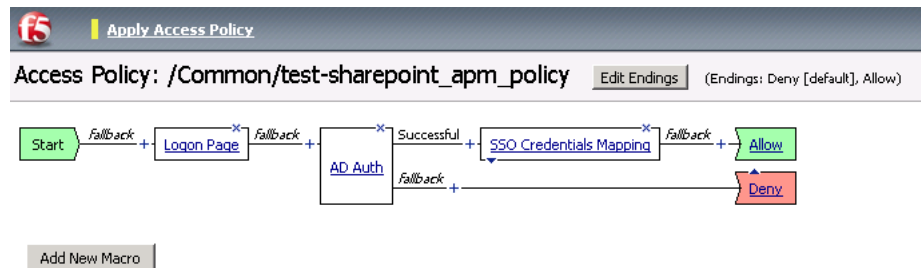
Editing the Access Policy

In the following procedure, we show you how to edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.

2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click the **Add Item** button.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click the **Save** button.
6. Click the **+** symbol on the between **Logon Page** and **Deny**.
7. Click **AD Auth** option button, and then click the **Add Item** button.
 - a. From the **Server** list, select the AAA server you configured in the table above.
 - b. All other settings are optional.
 - c. Click **Save**. You now see a Successful and Fallback path from AD Auth.
8. On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
9. Click the **SSO Credential Mapping** option button, and then click the **Add Item** button.
10. Click the **Save** button.
11. Click the **Deny** link in the box to the right of **SSO Credential Mapping**.
12. Click **Allow** and then click **Save**. Your Access policy should look like the example below.
13. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.
14. Click the **Close** button on the upper right to close the VPE.



Disabling Strict Updates

Before you can attach the Access Profile to the virtual server, you must disable Strict Updates.

To disable the Strict Updates feature

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your SharePoint Application service from the list.
3. From the **Application Service** menu, select **Advanced**.
4. In the **Strict Updates** row, clear the checkbox to disable Strict Updates.
5. Click **Update**.

Adding the Access Profile to the virtual server

The final task is to modify the virtual server created by the iApp to use the Access Profile you created in this section.

To modify the virtual server

1. On the Main tab, under **Local Traffic**, click **Virtual Servers**.
2. From the list, locate the main SharePoint virtual server created by the iApp. This is prefaced by the name you gave the iApp, followed by either **_http** (if you are not offloading SSL) or **_https** (if you are offloading SSL).
3. In the Access Policy section, from the Access Profile list, select the name of the Access Profile you created using the table.
4. Click **Update**.

This completes the BIG-IP APM configuration.

Optional: Configuring SSL Bridging on the BIG-IP LTM

One feature that is not yet part of the iApp template is the ability to for the BIG-IP LTM to re-encrypt SSL traffic after processing it (SSL Bridging). If you have configured your SharePoint web application to use Basic authentication, user passwords are sent in clear text between the BIG-IP system and SharePoint servers. F5 recommends configuring BIG-IP for SSL bridging in this scenario.

Configuring the iApp template to support SSL bridging

When you are configuring the iApp template, use the following guidance for SSL Bridging.

- Select **Yes** to the question *Do you want the BIG-IP system to offload SSL processing from the SharePoint servers?*
- If you have configured the SharePoint servers to use Basic authentication, select **No** to the question *Are the SharePoint servers configured to use NTLM authentication?*

Additional prerequisites

The following items must be completed before configuring SSL Bridging,

- Make sure you have configured Alternate Access Mappings as described in *Configuring SharePoint Alternate Access Mappings to support SSL offload on page 5*.
- Confirm you can access to the SharePoint application through the BIG-IP system.
- On each IIS server that is a member of the SharePoint pool, open **IIS Manager** and then highlight the web site that corresponds to your web application. From the task pane, click **Bindings**. Add a binding for port **443** listening on all IP addresses and select a certificate to use for HTTPS access to the SharePoint web application. This must be the same certificate used in the BIG-IP LTM configuration, and must have all of the host names of the SharePoint Pool member servers added to it in the Subject Alternative Name field. Finally, restart IIS. For more information on configuring IIS, consult the Microsoft documentation.

Configuring the BIG-IP LTM to support SSL Bridging

Use the following procedures to configure SSL Bridging on the LTM.

Disabling the Strict Updates feature

Before modifying the configuration produced by the iApp, you must turn off the Strict Updates feature. By turning off Strict Updates, if you re-enter the iApp template and modify the configuration within the iApp, you will have to make all of the following changes again manually. A future version of the template will contain these modifications.

To turn off Strict Updates

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your SharePoint 2010 Application service from the list.
3. From the **Application Service** list, select **Advanced**.
4. In the **Strict Updates** row, clear the check from the box to disable Strict Updates.
5. Click the **Update** button.

Creating a new health monitor on port 443

The next task is to create a new HTTPS health monitor. Before creating this monitor, we recommend opening the existing HTTP monitor for SharePoint (this monitor is preceded by the name you gave the iApp, followed by **_http_monitor**) making note of the settings, particularly the Interval and Timeout values, and the Send and Receive Strings.

To create a new HTTPS monitor

1. On the Main tab, expand **Local Traffic** and then click **Monitors**.
2. Click the **Create** button.
3. In the **Name** box, type a unique name, such as **my_sharepoint_https_monitor**.
4. Configure the properties of the monitor the same way as the HTTP monitor created by the template. If you left the default values in the iApp, the only settings you need to change are setting the *Interval* to **30** and *Timeout* to **91**.
If you configured custom Send and Receive Strings, be sure to include those values.
5. Click **Finished**.

Modifying the SharePoint Pool created by the iApp

The next task is to modify the SharePoint pool to use the new monitor you created, add new members on port 443, and remove the existing members on port 80.

To modify the members of the SharePoint pool

1. On the Main tab, expand **Local Traffic** and then click **Pools**.
2. From the list, click the name of the SharePoint pool created by the iApp. This pool is preceded by the name you gave the iApp, followed by **_pool**. The Pool Properties page opens.
3. In the Health Monitor section, from the **Active** list, select the HTTP monitor created by the template and then click the Remove (>>) button.
4. From the **Available** list, select the new HTTPS monitor you created and then click the Add (<<) button to move it to the Active list.
5. Click the **Update** button.
6. On the Menu bar, click **Members**.
7. In the Current Members section, click the Add button. The New Pool Members page opens.
8. In the **Address** box, type one of the addresses of your SharePoint servers. This address should match an IP address of an existing member.
9. In the **Service Port** box, type **443**, or select **HTTPS** from the list. Other settings are optional.
10. Click the **Repeat** button and repeat steps 5 and 6 for each existing pool member. When you have completed all addresses, click the **Finished** button. You return to the Members page.
11. From the Current Members table, check the boxes for all members on port 80, and then click the **Remove** button.

Adding a Server SSL profile to the virtual server

The final task is to add a server SSL profile to the SharePoint HTTPS virtual server.

To add a server SSL profile to the SharePoint virtual server

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the list, click the name of the SharePoint HTTPS virtual server created by the iApp. This pool is preceded by the name you gave the iApp, followed by **_https**.
3. From the **Server SSL** list, select **serverssl**.
4. Click **Update**.

This completes the configuration. Verify you can still access the SharePoint application through the BIG-IP system.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for SharePoint 2010. Advanced users extremely familiar with the BIG-IP system can use the following tables to manually configure the BIG-IP system. These tables contain a list of BIG-IP configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (Main tab-->Local Traffic-->Monitors)	Name	Type a unique name	
	Type	HTTP (HTTPS if you require SSL Bridging. See <i>Optional: Configuring SSL Bridging on the BIG-IP LTM on page 18)</i>	
	Interval	30 (recommended)	
	Timeout	91 (recommended)	
Pool (Main tab-->Local Traffic -->Pools)	Name	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time¹	300	
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)	
	Address	Type the IP Address of the SharePoint nodes	
	Service Port	80 (443 if configuring SSL Bridging). Click Add to repeat Address and Service Port for all nodes)	
Profiles (Main tab-->Local Traffic-->Profiles)	HTTP (Profiles-->Services)	Name	Type a unique name
		Parent Profile	http
		Rewrite Redirect ²	Matching²
	TCP WAN (Profiles-->Protocol)	Name	Type a unique name
		Parent Profile	tcp-wan-optimized
	TCP LAN (Profiles-->Protocol)	Name	Type a unique name
		Parent Profile	tcp-lan-optimized
	Persistence (Profiles-->Persistence)	Name	Type a unique name
		Persistence Type	Cookie
	OneConnect (Profiles-->Other)	Name	Type a unique name
Parent Profile		oneconnect	
NTLM² (Profiles-->Other)	Name	Type a unique name	
	Parent Profile	ntlm²	
Client SSL³ (Profiles-->SSL)	Name	Type a unique name	
	Parent Profile	clientssl	
	Certificate and Key	Select the Certificate and Key you imported	
Web Acceleration (Profiles-->Services)	Name	Type a unique name	
	Parent Profile	optimized-caching	
HTTP Compression (Profiles-->Services)	Name	Type a unique name	
	Parent Profile	wan-optimized-compression	
	Content List -->Include List (Add each entry to the Content Type box and then click Include)	application/vnd.ms-publisher	
		application/(xls excel msexcel ms-excel x-excel x-xls xmsexcel x-ms-excel)vnd.excel vnd.msexcel vnd.ms-excel)	
		application/(word doc mword winword ms-word x-word x-msword)vnd.word vnd.msword vnd.ms-word)	
		application/(xml x-javascript javascript x-ecmascript ecmascript)	
		application/(powerpoint mspoverpoint ms-powerpoint x-powerpoint x-mspowerpoint vnd.powerpoint vnd.ms-powerpoint vnd.ms-powerpoint vnd.ms-pps)	
		application/(mpp msproject x-msproject x-ms-project vnd.ms-project)	
		application/(visio x-visio vnd.visio vsd x-vsdx vnd)	
		application/(pdf x-pdf acrobat vnd.pdf)	

¹ You must select **Advanced** from the **Configuration** list for these options to appear
² An NTLM profile is only required when using NTLM authentication **and** OneConnect.
³ Only required if offloading SSL on the BIG-IP LTM

This table continues on the following page

Configuration table, continued: Optional Module configuration

BIG-IP ASM Object	Non-default settings/Notes		
ASM Configuration (Main tab-->Application Security) <i>Optional</i>	HTTP Class Profile (Local Traffic--> Profiles-->Protocol)	Name Parent Profile Application Security WebAccelerator¹	Type a unique name httpclass Enabled If you are also using the BIG-IP WebAccelerator, select Accelerate from the list.
	ASM Security Policy (Application Security--> Web Applications)	Web Applications list Security Policy Deployment Wizard	From the Web Application table, find the HTTP class you created above, and then in the Active Security Policy column, click Configure Security Policy . Follow the Security Policy wizard with information appropriate for your configuration.
BIG-IP WAM Object	Non-default settings/Notes		
WebAccelerator Configuration (Main tab--> WebAccelerator) <i>Optional</i>	WebAccelerator Application (WebAccelerator--> Applications)	Application Name Central Policy Requested Host	Type a unique name Microsoft SharePoint 2010 Type the Fully Qualified Domain Name (FQDN) of your application. Click Add Host to add additional hosts.
	Web Acceleration Profile (Profiles-->Services)	Name Parent Profile WA Applications	Type a unique name webacceleration Enable the WebAccelerator Application you created above

¹ Optional, only necessary if you are deploying both ASM and WebAccelerator.

BIG-IP APM configuration

If you are using the BIG-IP APM, see *Configuring BIG-IP Access Policy Manager for SharePoint 2010 on page 15* to create the APM objects and edit the Access Profile. You do not need to disable Strict Updates or modify the virtual server.

This table continues on the following page

BIG-IP LTM Object	Non-default settings/notes	
Virtual Servers (Main tab-->Local Traffic -->Virtual Servers)	HTTP	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	80
	Protocol Profile (client)^{1,2}	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)^{1,2}	Select the LAN optimized TCP profile you created above
	OneConnect²	Select the OneConnect profile you created above
	HTTP Profile²	Select the HTTP profile you created above
	NTLM^{2,3}	If applicable, select the NTLM profile you created above
	Web Acceleration profile²	Select the Web Acceleration profile you created above
	HTTP Compression profile²	Select the HTTP Compression profile you created above
	SNAT Pool⁴	Automap (optional; see footnote ⁴)
	Access Profile^{2,7}	Select the Access profile you created above for APM
	Default Pool²	Select the pool you created above
	Persistence Profile²	Select the Persistence profile you created
	iRule⁵	If offloading SSL only: Enable the built-in _sys_https_redirect iRule
	HTTPS⁶	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	443
	Protocol Profile (client)¹	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)¹	Select the LAN optimized TCP profile you created above
	OneConnect	Select the OneConnect profile you created above
	HTTP Profile	Select the HTTP profile you created above
	NTLM^{2,3}	If applicable, select the NTLM profile you created above
	Web Acceleration profile	Select the Web Acceleration profile you created above. Note: If you are using WebAccelerator, be sure to select the profile you created in the WebAccelerator configuration table with the webacceleration parent.
HTTP Compression profile	Select the HTTP Compression profile you created above	
SSL Profile (Client)	Select the Client SSL profile you created above	
SSL Profile (Server)⁸	serverssl⁸	
SNAT Pool⁴	Automap (optional; see footnote ⁴)	
Access Profile⁷	Select the Access profile you created above for APM	
HTTP Class Profiles	<i>If you are using ASM only:</i> Enable the HTTP Class profile you created in the ASM configuration table.	
Default Pool	Select the pool you created above	
Persistence Profile	Select the Persistence profile you created	

¹ You must select **Advanced** from the **Configuration** list for these options to appear

² Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.

³ Only necessary if using NTLM and OneConnect. You must first select an HTTP profile before you can select a NTLM profile

⁴ If want to use SNAT, and you have a large SharePoint deployment expecting more than 8,000 simultaneous users, you must configure a SNAT Pool with an IP address for each 8,000 simultaneous users you expect. See the BIG-IP documentation on configuring SNAT Pools.

⁵ Only enable this iRule if offloading SSL

⁶ Only create this virtual server if offloading SSL

⁷ Only necessary if using BIG-IP APM and you have created an Access Profile

⁸ Only necessary if configuring SSL Bridging

Appendix B: Configuring DNS and NTP on the BIG-IP system

If you are using the BIG-IP APM, you must have DNS and NTP settings configured on the BIG-IP system. If you do not, use the following procedures.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to the Active Directory server.

➤ **Note:** *DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.*

➤ **Important:** *The BIG-IP system must have a Route to the Active Directory server. The Route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a Route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
 - a. In the **Address** box, type the IP address of a DNS server that can resolve the Active Directory server.
 - b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the BIG-IP command line, run **ntpq -np**.

See <http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html> for more information on this command.

Document Revision History

Version	Description	Date
1.0	New Version	N/A
1.1	Added link to the Microsoft FAST Search Server 2010 for SharePoint 2010	N/A
2.0	- Added manual configuration for BIG-IP Access Policy Manager - Updated the manual configuration tables to include Application Security Manager and WebAccelerator configuration	N/A
2.1	Added instructions for configuring SharePoint Alternate Access Mappings if offloading SSL on the BIG-IP system.	3-26-2012
2.2	Added additional instructions to the Alternate Access Mappings section for ensuring the search results are properly displayed for HTTPS queries.	4-2-2012
2.3	Added instructions for configuring SSL Bridging: <i>Optional: Configuring SSL Bridging on the BIG-IP LTM on page 18</i> . Also added the SSL Bridging options to the manual configuration tables.	4-26-2012

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

