Deploying the BIG-IP System with Microsoft SharePoint

Welcome to the F5 deployment guide for Microsoft® SharePoint®. This document contains guidance on configuring the BIG-IP system version 11.4 and later for Microsoft SharePoint 2010 and 2013 implementations, resulting in a secure, fast, and available deployment. This guide shows how to quickly and easily configure the BIG-IP system using the SharePoint iApp Application template. There is also an appendix with manual configuration tables for users who prefer to create each individual object.

Note: There is now a Release Candidate iApp template available for this solution which contains important fixes. See *http://www.f5.com/pdf/deployment-guides/iapp-sharepoint-2010-2013-dg-rc1.pdf* for information and instructions.

Why F5?

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

- F5 can reduce the burden on servers by monitoring SharePoint Server responsiveness across multiple ports and protocols, driving intelligent load balancing decisions.
- 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.
- Access Policy Manager enables secure mobile device access management, as well as pre-authentication to SharePoint.
- CPU-intensive operations such as compression, caching, and SSL processing can be offloaded onto the BIG-IP system, which can extend SharePoint Server capacity by 25%.
- F5 WAN optimization technology can dramatically increase SharePoint 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. This includes using the iApp template to deploy the BIG-IP Advanced Firewall Manager.
- F5 can be used as a reverse proxy alternative to TMG.

Products and applicable versions

Product	Versions
BIG-IP LTM, AAM, APM, ASM, AFM	11.4, 11.4.1, 11.5, 11.5.1, 11.6
Microsoft SharePoint	2010, 2013
iApp version	f5.microsoft_sharepoint_2010_2013.v1.1.0
Deployment guide version	1.6 (see *Document Revision History on page 62*)

Microsoft® Partner Network™

Contents

Visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: *http://devcentral.f5.com/Microsoft/*.

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/iapp-sharepoint-2010-2013-dg.pdf*

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

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 these servers.

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:

- This document provides guidance on using the **downloadable iApp** for Microsoft SharePoint 2010 and 2013 available via *http://support.f5.com/kb/en-us/solutions/public/15000/000/sol15043.html*, and **not** the iApp found by default in BIG-IP version 11. ***You must use this downloadable iApp for BIG-IP versions 11.4 and later*** as it contains a number of fixes and enhancements not found in the default iApp, or other downloadable versions.
- For this guide, the BIG-IP system ***must*** be running version 11.4 or later. If you are using a previous version of the BIG-IP system, see the deployment guide index on *F5.com*. The configuration described in this guide does not apply to previous versions.
- If you upgraded the BIG-IP system from a previous version, and have an existing Application Service that used the f5.microsoft_sharepoint_2010 iApp template, see *Upgrading an Application Service from previous version of the iApp template on page 10*.
- See *Troubleshooting on page 38* for important troubleshooting tips if you are experiencing deployment issues.
- This deployment guide provides guidance for using the iApp for Microsoft SharePoint found in version 11.4 and later. For users familiar with the BIG-IP system, there is a manual configuration table at the end of this guide. However, because the configuration can be complex, we recommend using the iApp template.
- If you are using the BIG-IP system to offload SSL or for SSL Bridging, we assume you have already obtained the appropriate SSL certificate and key, and it is installed on the BIG-IP LTM system.
- If you are using the BIG-IP Application Acceleration Manager (AAM) for Symmetric optimization between two BIG-IP systems (optional), you must have pre-configured the BIG-IP AAM for Symmetric Optimization using the Quick Start wizard or manually configured the necessary objects. See the BIG-IP AAM documentation (*http://support.f5.com/kb/en-us/products/big-ip-aam.html*) for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.
- If you are configuring the BIG-IP system for SharePoint 2013 and have enabled Request Management in dedicated mode, you should specify the Request Management farm server IP addresses when configuring the pool members section of the iApp.
  If you have enabled Request Management in integrated mode, be aware that Request Management routing and throttling rules will override the load balancing decisions of the BIG-IP system. For this reason, F5 recommends choosing the Least Connections load balancing mode for both dedicated and integrated Request Management deployments.
- 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 *Appendix A: Configuring SharePoint Alternate Access Mappings to support SSL offload on page 42.*

- If you are deploying Microsoft Office Web Apps Server 2013 with SharePoint 2013, there are important instructions and modifications to make to this configuration. See *http://www.f5.com/pdf/deployment-guides/microsoft-office-web-apps-dg.pdf*.

- If you are deploying SharePoint 2013 and SharePoint Apps, you must configure the BIG-IP system (either using the iApp or manually) for SSL Bridging. See *Modifying the iApp configuration on page 31.*

- 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*

- If you are not using split DNS, and requests from the SharePoint 2010 front end servers to the SharePoint URL are routed through the external SharePoint virtual server on the BIG-IP LTM you may see problems with missing page images, or issues loading or clicking the SharePoint ribbon when a request from the WFE server is load balanced to another server rather than to itself. See the additional section, *Troubleshooting on page 38* for instructions.

- If you are deploying BIG-IP APM, and want to support smart card authentication, the following are prerequisites:
    - The SharePoint web application must be configured for Kerberos authentication;
    - A delegation account must be created in the AD domain to allow the BIG-IP system to authenticate on behalf of the user;
    - Service Principal Names (SPNs) must be correctly configured for the BIG-IP APM delegation account;
    - Kerberos constrained delegation must be enabled for the BIG-IP APM delegation account;
    - Forward and reverse DNS zones must be configured and contain A and PTR records for SharePoint server(s), respectively.

Optional Modules

This Microsoft SharePoint iApp allows you to use four optional modules on the BIG-IP system. To take advantage of these modules, they must be licensed and provisioned before starting the iApp template. For more information on licensing modules, contact your sales representative.

- **BIG-IP AAM** (formerly BIG-IP WAN Optimization Manager and WebAccelerator)
  BIG-IP AAM provides application, network, and front-end optimizations to ensure consistently fast performance for today's dynamic web applications, mobile devices, and wide area networks. With sophisticated execution of caching, compression, and image optimization, BIG-IP AAM decreases page download times. You also have the option of using BIG-IP AAM for symmetric optimization between two BIG-IP systems. For more information on BIG-IP Application Acceleration Manager, see *https://f5.com/products/modules/application-acceleration-manager*.

- **BIG-IP ASM**
  BIG-IP ASM protects the People applications your business relies on with an agile, certified web application firewall and comprehensive, policy-based web application security. Offering threat assessment and mitigation, visibility, and almost limitless flexibility, BIG-IP ASM helps you secure your PeopleSoft applications. For more information on BIG-IP Application Security Manager, see *https://f5.com/products/modules/application-security-manager*.

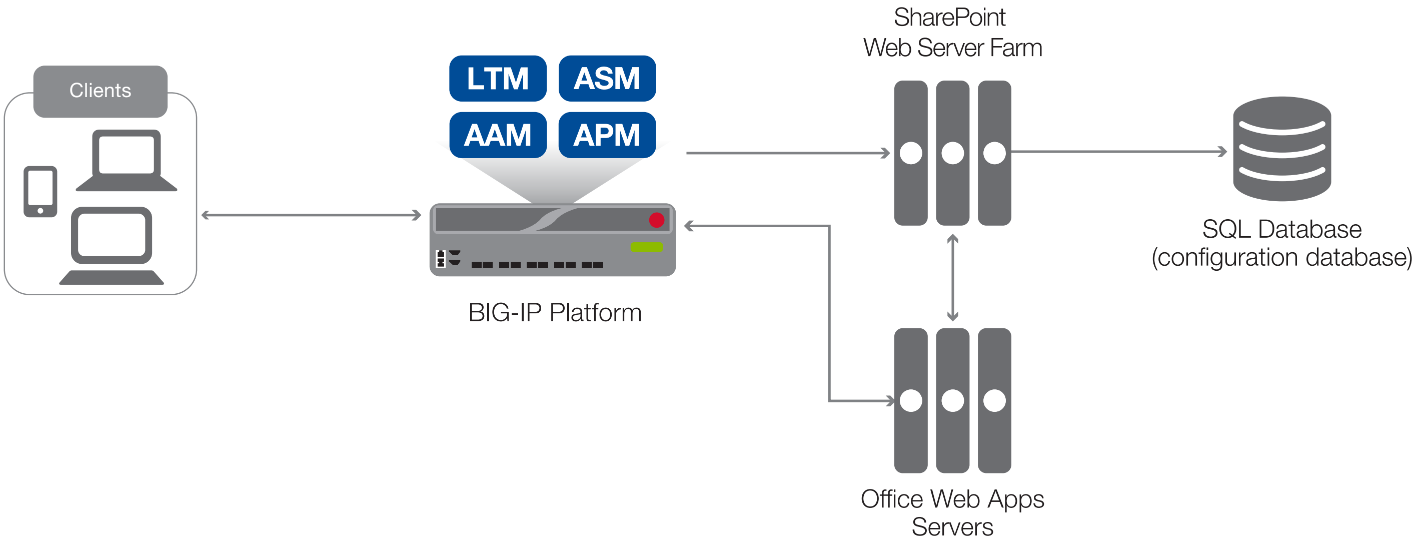
- **BIG-IP APM**
  BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your business-critical applications and networks. By consolidating remote access, web access management, VDI, and other resources in a single policy control point—and providing easy-to-manage access policies—BIG-IP APM helps you free up valuable IT resources and scale cost-effectively. For more information on BIG-IP APM, see *https://f5.com/products/modules/access-policy-manager*.

- **BIG-IP AFM**
  BIG-IP Advanced Firewall Manager (AFM) is a high-performance, stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols—including HTTP/S, SMTP, DNS, and FTP. By aligning firewall policies with the applications they protect, BIG-IP AFM streamlines application deployment, security, and monitoring. For more information on BIG-IP AFM, see *https://f5.com/products/modules/advanced-firewall-manager*.

- **Application Visibility and Reporting**
  F5 Analytics (also known as Application Visibility and Reporting or AVR) is a module on the BIG-IP system that lets customers view and analyze metrics gathered about the network and servers as well as the applications themselves. Making this information available from a dashboard-type display, F5 Analytics provides customized diagnostics and reports that can be used to optimize application performance and to avert potential issues. The tool provides tailored feedback and recommendations for resolving problems. Note that AVR is licensed on all systems, but must be provisioned before beginning the iApp template.

Configuration scenarios

Using the iApp template for Microsoft SharePoint, it is extremely easy to optimally configure the BIG-IP system to optimize and direct traffic to Microsoft SharePoint servers. Using the options found in the iApp and the guidance in this document, you can configure the BIG-IP system for a number of different scenarios. This section details just a few of the options.


Clients
LTM
ASM
AAM
APM
BIG-IP Platform
SharePoint Web Server Farm
SQL Database (configuration database)
Office Web Apps Servers

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 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, BIG-IP AAM 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 AAM, the AAM 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.

Microsoft Office Web Apps Server configuration

9. The client requests a preview of Office documents in a web browser.
10. SharePoint 2013 server(s) send request to Office Web Apps server(s).
11. Office Web Apps server(s) request content from SharePoint 2013 farm.
12. SharePoint 2013 server(s) render content from Office Web Apps server(s) to client in a separate browser window.

Configuring the BIG-IP system as reverse (or inbound) proxy

In its traditional role, the BIG-IP system is a reverse proxy. The system is placed in the network between the clients and the servers. Incoming requests are handled by the BIG-IP system, which interacts on behalf of the client with the desired server or service on the server. This allows the BIG-IP system to provide scalability, availability, server offload, and much more, all completely transparent to the client.

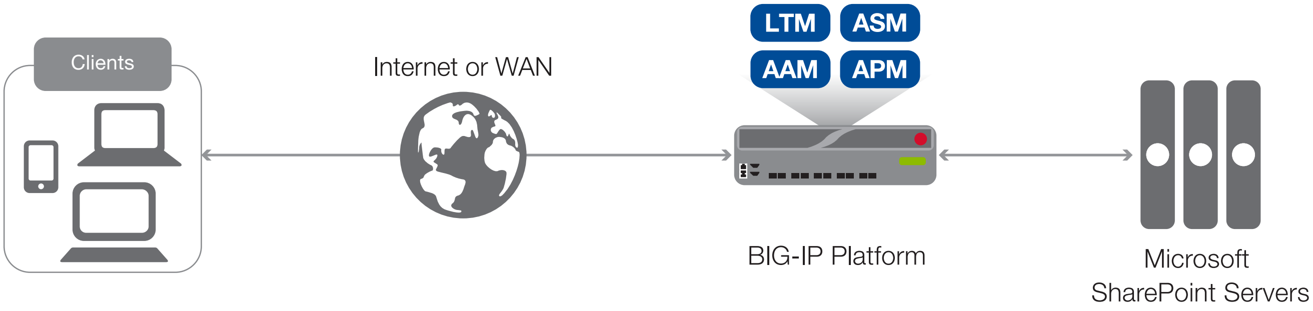


Figure 1: *Using the BIG-IP system as a reverse proxy*

To configure this scenario

There are no questions in the iApp template that you must answer in a specific way for the BIG-IP system to act as a reverse proxy, the BIG-IP system acts as a reverse proxy by default.

Accelerating application traffic over the WAN

The iApp enables you to use the BIG-IP system's Application Acceleration Manager module to optimize and secure your web traffic over the WAN (wide area network). The iApp uses the default *iSession profile* to create a secure tunnel between BIG-IP systems to accelerate and optimize the traffic.

In this scenario, you must have a symmetric BIG-IP deployment (as shown in Figure 2), with a BIG-IP system between your clients and the WAN, and another between the WAN and your SharePoint servers. You run the iApp template on each of the BIG-IP systems, using the settings found in the following table.

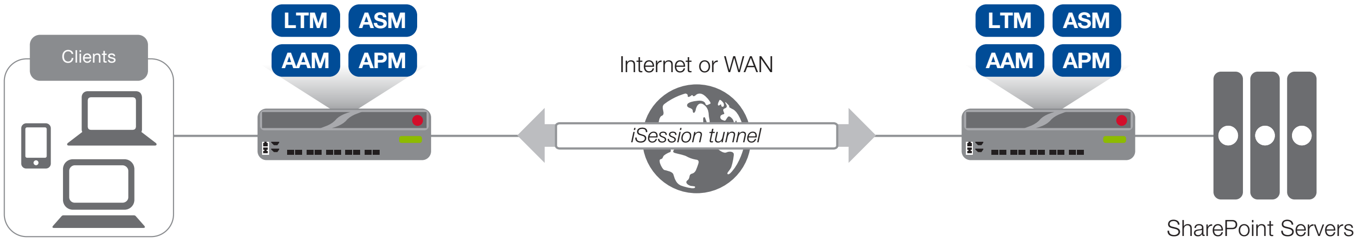


Figure 2: *Using an iSession tunnel to secure and optimize traffic between two BIG-IP systems*

To configure this scenario

If you select this option, you must have already configured the BIG-IP AAM for Symmetric Optimization as mentioned in the prerequisites. See the BIG-IP AAM documentation available on Ask F5 (*http://support.f5.com/kb/en-us/products/big-ip-aam.html*) for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

To configure the system for this scenario, at a minimum you must answer the following questions with the appropriate answers in the iApp template as shown in the following table.

The following table assumes you are configuring the BIG-IP system on the client side of the WAN.

iApp template question	Your answer
On the BIG-IP system between clients and the WAN	
What type of network connects clients to the BIG-IP system? (on page 12)	**LAN** or **WAN** as appropriate
What type of network connects servers to the BIG-IP system? (on page 13)	**WAN through another BIG-IP system**
Do you want to create a new pool or use an existing one?	Typically you would leave this at the default (Do not use a pool), however you could create a pool of local servers as a fallback in case the WAN becomes unavailable.
On the BIG-IP system between servers and the WAN	
What type of network connects clients to the BIG-IP system? (on page 12)	**WAN through another BIG-IP system**
What type of network connects servers to the BIG-IP system? (on page 13)	**LAN** or **WAN** as appropriate (Typically LAN)

Using the BIG-IP system with SSL traffic

The Microsoft SharePoint iApp template provides the following options for dealing with encrypted traffic:

- **SSL offload**
  When performing SSL offload, the BIG-IP system accepts incoming encrypted traffic, decrypts (or terminates) it, and then sends the traffic to the servers unencrypted. By saving the servers from having to perform the decryption duties, F5 improves server efficiency and frees server resources for other tasks. SSL certificates and keys are stored on the BIG-IP system.
- **SSL bridging**
  With SSL Bridging, also known as SSL re-encryption, the BIG-IP system accepts incoming encrypted traffic, decrypts it for processing, and then re-encrypts the traffic before sending it back to the servers. This is useful for organizations that have requirements for the entire transaction to be SSL encrypted. In this case, SSL certificates and keys must be are stored and maintained on the BIG-IP system and the SharePoint servers.
- **SSL pass-through**
  With SSL pass-through, the BIG-IP system does not process the encrypted traffic at all, just sends it on to the servers.
- **No SSL (plaintext)**
  In this scenario, the BIG-IP system does not perform any SSL processing, as all traffic is only plaintext.
- **Server-side encryption**
  In this scenario, the BIG-IP system accepts unencrypted traffic and then encrypts is before sending it to the servers. While more uncommon than offload or bridging, this can be useful for organizations that require all traffic behind the system to be encrypted.

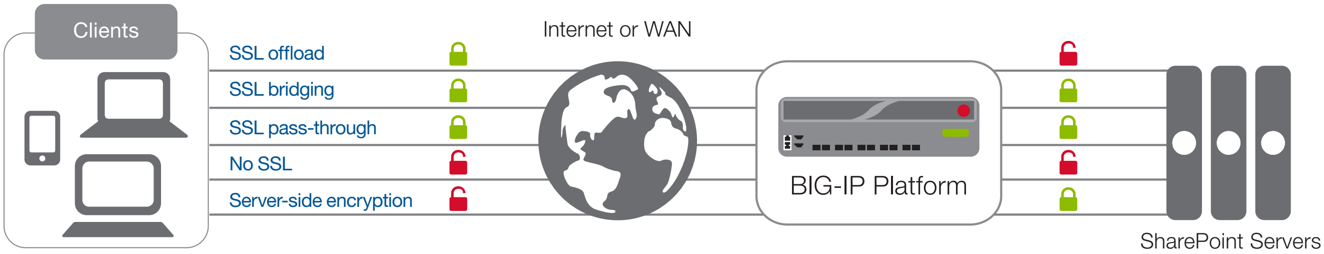


Figure 3: *SSL options*

To configure these scenarios

For SSL offload or SSL bridging, you must have imported a valid SSL certificate and key onto the BIG-IP system. Importing certificates and keys is not a part of the template, see **System > File Management > SSL Certificate List**, and then click **Import**.

iApp template question	Your answer	
How should the BIG-IP system handle SSL traffic (on page 17)	Select the appropriate option for your configuration:	
	SSL offload:	**Encrypt to clients, plaintext to servers**
	SSL bridging:	**Terminate SSL from clients, re-encrypt to servers**
	SSL pass-through	**Encrypted traffic is forwarded without decryption**
	No SSL:	**Plaintext to clients and servers**
	Server-side encryption:	**Plaintext to clients, encrypt to servers**

Using this guide

This deployment guide is intended to help users deploy web-based applications using the BIG-IP system. This document contains guidance configuring the BIG-IP system using the iApp template, as well as manually configuring the BIG-IP system.

Using this guide to configure the iApp template

We recommend using the iApp template to configure the BIG-IP system for your Microsoft SharePoint implementation. The majority of this guide describes the iApp template and the different options the template provides for configuring the system for Microsoft SharePoint.

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or inline help. The questions in the UI for the iApp template itself are all displayed in a table and at the same level. In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. ***Top-level question found in the iApp template***
    - ***Select an object you already created from the list*** (such as a profile or pool; not present on all questions. Shown in bold italic)
    - **Choice #1** (in a drop-down list)
    - **Choice #2** (in the list)
        a. *Second level question dependent on selecting choice #2*
            - **Sub choice #1**
            - **Sub choice #2**
                i). *Third level question dependent on sub choice #2*
                    - **Sub-sub choice**
                    - **Sub-sub #2**
                        1). *Fourth level question (rare)*

Advanced options/questions in the template are marked with the Advanced icon: **Advanced**. These questions only appear if you select the Advanced configuration mode.

Using this guide to manually configure the BIG-IP system

Users already familiar with the BIG-IP system can use the manual configuration tables to configure the BIG-IP system for the SharePoint implementation. These configuration tables only show the configuration objects and any non-default settings recommended by F5, and do not contain procedures on specifically how to configure those options in the Configuration utility. See *Appendix B: Manual configuration tables on page 45.*

Preparing to use the iApp

In order to use the iApp for Microsoft SharePoint, it is helpful to have some information, such as server IP addresses and domain information before you begin. Use the following table for information you may need to complete the template. The table includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

BIG-IP system Preparation Table		
Basic/Advanced mode	In the iApp, you can configure the system for Microsoft SharePoint with F5 recommended settings (Basic mode) which are a result of extensive testing and tuning with Microsoft SharePoint. Advanced mode allows configuring the BIG-IP system on a much more granular level, configuring specific options, or using your own pre-built profiles or iRules. Basic/Advanced "configuration mode" is independent from the Basic/Advanced list at the very top of the template which only toggles the Device and Traffic Group options (see page 11)	
Network	**Type of network between clients and BIG-IP**	**Type of network between servers and BIG-IP**
	LAN | WAN | WAN through another BIG-IP system	LAN | WAN | WAN through another BIG-IP system
	If WAN through another BIG-IP system, you must have BIG-IP AAM pre-configured for Symmetric Optimization.	
	Where are BIG-IP virtual servers in relation to the servers	**Expected number of concurrent connections per server**
	Same subnet | Different subnet	More than 64k concurrent | Fewer than 64k concurrent
	If they are on different subnets, you need to know if the SharePoint servers have a route through the BIG-IP system. If there is not a route, you need to know the number of concurrent connections.	If more than 64k per server, you need an available IP address for each 64k connections you expect for the SNAT Pool
SSL Encryption	**SSL Offload or SSL Bridging**	**Re-encryption (Bridging and server-side encryption)**
	If configuring the system for SSL Offload or SSL Bridging, you must have imported a valid SSL certificate and key onto the BIG-IP system. You have the option of also using an Intermediate (chain) certificate as well if required in your implementation. *Certificate:* *Key:* *Intermediate Certificate (optional):*	When the BIG-IP system encrypts traffic to the servers, it is acting as an SSL client and by default we assume the servers do not expect the system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must create a custom Server SSL profile outside of the template with the appropriate certificate and key.
Virtual Server and Pools	**Virtual Server**	**SharePoint server pool**
	The Virtual server is the address clients use to access the servers.	The *load balancing pool* is the LTM object that contains the servers.
	IP address for the virtual server: *Associated service port:* *FQDN clients will use to access the Microsoft SharePoint servers:*	*IP addresses of the servers:* 1: 2: 3: 4: 5: 6: 7: 8: 9:
Profiles	For each of the following *profiles*, the iApp will create a profile using the F5 recommended settings (or you can choose 'do not use' many of these profiles). While *we recommend using the profiles created by the iApp*, you have the option of creating your own custom profile outside the iApp and selecting it from the list. The iApp gives the option of selecting our the following profiles (some only in Advanced mode). Any profiles must be present on the system before you can select them in the iApp	
	HTTP | Persistence | HTTP Compression | TCP LAN | TCP WAN | OneConnect | Web Acceleration | NTLM | iSession	
Health monitor	**HTTP Request**	**User Account**
	In Advanced mode, you have the option of selecting the type of HTTP request the health monitor uses: GET or POST. You can also specify Send and Receive strings to more accurately determine server health. *Send string* (the URI sent to the servers)*:* *Receive string* (what the system expects in return)*:* *POST Body* (only if using POST)*:*	Also in advanced mode, the monitor can attempt to authenticate to the SharePoint servers as a part of the health check. If you want the monitor to require credentials, create a user account specifically for this monitor that has no additional permissions and is set to never expire. Account maintenance becomes a part of the health monitor, as if the account is deleted or otherwise changed, the monitor will fail and the servers will be marked down.
BIG-IP AAM	You can optionally use the BIG-IP Application Acceleration Manager (AAM) module to help accelerate your SharePoint traffic. To use BIG-IP AAM, it must be fully licensed and provisioned on your BIG-IP system. Consult your F5 sales representative for details. If you are using BIG-IP AAM, and want to use a custom Web Acceleration policy, it must have an Acceleration policy attached.	
BIG-IP ASM and AFM	You can optionally use the BIG-IP ASM and AFM modules to help protect and secure your SharePoint deployment. To use either module, it must be fully licensed and provisioned on your BIG-IP system. Consult your F5 sales representative for details.	
iRules	In Advanced mode, you have the option of attaching iRules you create to the virtual server created by the iApp. For more information on iRules, see *https://devcentral.f5.com/irules*. Any iRules you want to attach must be present on the system at the time you are running the iApp.	

Configuring the BIG-IP iApp for Microsoft SharePoint

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

Downloading and importing the new iApp

The first task is to download and import the new SharePoint 2010 and 2013 iApp template.

To download and import the iApp

1. Open a web browser and go to *http://support.f5.com/kb/en-us/solutions/public/15000/000/sol15043.html*.
2. Follow the instructions to download the Microsoft SharePoint iApp to a location accessible from your BIG-IP system.
3. Extract (unzip) the **f5.microsoft_sharepoint_2010_2013v<latest version>.tmpl** file.
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

Upgrading an Application Service from previous version of the iApp template

If you upgraded your BIG-IP system from previous version and had an existing Application Service that used the f5.microsoft_sharepoint_2010 template from one of those versions, you will see a warning that the source template has changed. In version 11.4 and later, the iApp template for SharePoint has been significantly improved, and we strongly recommend you upgrade the source template to the new template available in v11.4 or later.

When you upgrade to the current template version, the iApp retains all of your settings for use in the new template. You will notice the location of the questions are different in the new version of the template, most questions are asked in a different way, and BIG-IP WebAccelerator is now called BIG-IP Application Acceleration Manager. There are also many more options you can configure in the new version of the template.

To upgrade an Application Service to the current version of the template

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the list, click the name of the Application Service you created using the f5.microsoft_sharepoint_2010 template.
3. On the Menu bar, click **Reconfigure**.
4. In the Template Options section, from the **Do you want to upgrade this template** question, select **Yes**.
5. Without changing any settings, click the **Finished** button. The system creates an Application Service object with only the new template object in the Component view.

   ⚠ ***Warning***

   Your application will be offline from now until you complete the process in step 9

6. On the Menu bar, click **Reconfigure**. Note the Template options section with inline help and configuration mode options. A number of additional questions appear if you select Advanced mode.
7. In the **Virtual Server and Pool** section, in the **What FQDNs will clients use to access the servers** question, you must add the host name.

8. No additional changes are necessary, but you may modify any of the other settings as applicable for your implementation. Use the inline help and this deployment guide for information on specific settings.
9. Click **Finished**. The upgrade is now complete and all applicable objects appear in the Component view.

Getting Started with the iApp for Microsoft SharePoint

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-iapp_.**
5. From the **Template** list, select **f5.microsoft_sharepoint_2010_2013.<latest version>**. The Microsoft SharePoint template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the top of the page, you see Device and Traffic Group 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. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.
2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.
   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method and parent profiles are all set automatically. The F5 recommended settings come as a result of extensive testing with web applications, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options like Slow Ramp Time and Priority Group Activation. You can also choose to attach iRules you have previously created to the Application Service. The Advanced option provides more flexibility for experienced users.

As mentioned, advanced options in the template are marked with the Advanced icon: Advanced . If you are using Basic/F5 recommended settings, you can skip the questions with the Advanced icon.

3. ***Which version of SharePoint are you deploying?***
Choose which version of Microsoft SharePoint you are using. The selection you make here determines some of the options that appear later in this template.

    - **SharePoint 2007 or 2010**
    Select this option if you are deploying this iApp template for SharePoint 2007 or 2010.

    - **SharePoint 2013**
    Select this option if you are deploying this iApp template for SharePoint 2013. In SharePoint 2013, the Distributed Cache service maintains authentication information across all SharePoint web application servers. Because of this, SharePoint 2013 does not require connections from a single client to persist to the same SharePoint server. So in order to get the maximum benefit from F5's OneConnect feature, the template removes the default persistence and NTLM profiles from the SharePoint 2013 BIG-IP virtual server, and changes the source mask value to 0.0.0.0 for the OneConnect profile.

Network

This section contains questions about your networking configuration.

1. ***What type of network connects clients to the BIG-IP system?***
Choose the type of network that connects your clients to the BIG-IP system. If you choose WAN or LAN, the BIG-IP system uses this information to determine the appropriate TCP optimizations. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN. Only choose this option if you have another BIG-IP system across the WAN that will be a part of this implementation.

    - **Local area network (LAN)**
    Select this option if most clients are connecting to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile which is optimized for LAN clients. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.

    - **Wide area network (WAN)**
    Select this option if most clients are connecting to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile which is optimized for WAN clients. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.

    - **WAN through another BIG-IP system**
    Select this option if client traffic is coming to this BIG-IP system from a remote BIG-IP system across a WAN. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

    If you select this option, you must have already initially configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

2. ***Do you want to restrict client traffic to specific VLANs?** (11.5 and later)* Advanced
***Which VLANs transport client traffic?** (11.4.x)* Advanced
The BIG-IP system allows you to restrict client traffic to specific VLANs that are present on the system. This can provide an additional layer of security, as you can allow or deny traffic from the VLANs you choose. By default, all VLANs configured on the system are enabled. If you select to enable or disable traffic on specific VLANs, you must specify the VLANs in the next question. The VLAN objects must already be configured on this BIG-IP system before you can select them.

    In version 11.4.x, you can only allow traffic from specific VLANs using the iApp template; v11.5 and later enables you to allow or deny client traffic from specific VLANs. If using v11.4.x, all allowed VLANs appear in the Selected list. Use the Move buttons (<<) and (>>) to adjust list membership. Only VLANs in the Selected list are allowed. With 11.4.x, you do NOT see the following options.

    - **Enable traffic on all VLANs and Tunnels**
    Choose this option to allow traffic from all VLANs and Tunnels. If you select this option, the question asking about VLANs disappears. Continue with #3.

- **Yes, enable traffic only on the VLANs I specify**
  Choose this option to restrict client traffic to specific VLANs that you specify in the following question. The system will accept SharePoint client traffic from these VLANs, and deny traffic from all other VLANs on the system.

  a. *On which VLANs should traffic be enabled or disabled?*
  Use this section to specify the VLANs that will accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so click the VLANs and then use the Move buttons (<<) and (>>) to adjust list membership.

  ➡ ***Note***

  If you choose to allow traffic from certain VLANs, when additional VLANs are added to the BIG-IP system at a later time, this iApp configuration will deny traffic from these VLANs by default. To accept traffic from these VLANs, you must re-enter the template and add the VLAN(s).

- **Yes, disable traffic only on the VLANs I specify**
  Choose this option to deny client traffic from the specific VLANs that you specify in the following question. The system will refuse SharePoint client traffic from these VLANs, and accept traffic from all other VLANs on the system.

  a. *On which VLANs should traffic be enabled or disabled?*
  Use this section to specify the VLANs that should not accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so it is critical in this case that you click the VLANs and then use the Move button (>>) to adjust list membership.

  ⚠ ***Warning***

  If you choose to disable certain VLANs, you must move at least one VLAN to the Options list. Otherwise, the system will deny traffic from all VLANs on the box, and the configuration, although valid, will not pass any traffic.

3. ***What type of network connects servers to the BIG-IP system?***
Choose the type of network that connects your servers to the BIG-IP system. Similar to the question about clients connecting to the BIG-IP system, if you choose WAN or LAN, the system uses this information to determine the appropriate TCP optimizations. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN. Only choose this option if you have another BIG-IP system across the WAN that will be a part of this Microsoft SharePoint implementation.

   - **Local area network (LAN)**
   Select this option if the servers connect to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.

   - **Wide area network**
   Select this option if the servers connect to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.

   - **WAN through another BIG-IP system**
   Select this option if servers are across a WAN behind another BIG-IP system. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

     If you select this option, you must have already initially configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

4. ***Where will the virtual servers be in relation to the SharePoint servers?***
Select whether your BIG-IP virtual servers are on the same subnet as your SharePoint servers, or on different subnets. This setting is used to determine the *SNAT* (secure NAT) and routing configuration.

   - **Virtual server IP and SharePoint servers are on the same subnet**
   If the BIG-IP virtual servers and SharePoint servers are on the same subnet, SNAT is configured on the BIG-IP virtual server and you must specify the number of concurrent connections.

a. *How many connections to you expect to each SharePoint server?*
Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

- **Fewer than 64,000 concurrent connections**
  Select this option if you expect fewer than 64,000 concurrent connections per SharePoint server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with *Virtual Server and Pools on page 21.*
- **More than 64,000 concurrent connections**
  Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

  i). *Create a new SNAT pool or use an existing one?*
  If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

  - **Create a new SNAT pool**
    Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

    1). *What are the IP addresses you want to use for the SNAT pool?*
    Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for more rows. Do not use any self IP addresses on the BIG-IP system.
  - **Select a SNAT pool**
    Select the SNAT pool you created for this deployment from the list.

    ⓘ ***Important***

    If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per SharePoint server is reached, new requests fail.

- **Virtual servers and SharePoint servers are on different subnets**
  If the BIG-IP virtual servers and servers are on different subnets, the following question appears.

a. *How have you configured routing on your SharePoint servers?*
If you chose different subnets, this question appears asking whether the SharePoint servers use this BIG-IP system's self IP address as their default gateway. Select the appropriate answer.

- **Servers have a route to clients through the BIG-IP system**
  Choose this option if the servers use the BIG-IP system as their default gateway. In this case, no configuration is needed to support your environment to ensure correct server response handling. Continue with the next section.
- **Servers do not have a route to clients through the BIG-IP system**
  If the SharePoint servers do not use the BIG-IP system as their default gateway, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

  i). *How many connections to you expect to each SharePoint server?*
  Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

  - **Fewer than 64,000 concurrent connections**
    Select this option if you expect fewer than 64,000 concurrent connections per SharePoint server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the *SSL Encryption* section.

- **More than 64,000 concurrent connections**
  Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections.

  1). *Create a new SNAT pool or use an existing one?*
  If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

  * **Create a new SNAT pool**
  Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

  a). *Which IP addresses do you want to use for the SNAT pool?*
  Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

  * **Select a SNAT pool**
  Select the SNAT pool you created for this deployment from the list.

  Important

  If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per SharePoint server is reached, new requests fail.

Access Policy Manager (BIG-IP APM)

The section in this scenario asks about the BIG-IP APM. You must have APM fully licensed and provisioned to use APM. If you are not deploying APM, continue with the next section. As mentioned in the prerequisites, if you are deploying APM, you must have configured the BIG-IP system for DNS and NTP. See *Appendix C: Configuring additional BIG-IP settings on page 56* for instructions.

Note

See page 40 for details about a Microsoft hotfix that corrects issues with opening SharePoint document libraries in Windows Explorer or editing Microsoft Office documents.

1. ***Provide secure authentication with BIG-IP Access Policy Manager?***
   Specify whether you want to deploy BIG-IP APM to provide proxy authentication and secure remote access for Microsoft SharePoint.

   ▶ **No, do not provide secure authentication using BIG-IP APM**
   Select this option if you do not want to use the BIG-IP APM at this time. You can always reconfigure the iApp template at a later date should you decide to add BIG-IP APM functionality.

   ▶ **Yes, provide secure authentication using BIG-IP APM**
   Select this option if you want to use the BIG-IP APM to provide proxy authentication and secure remote access for SharePoint.

   a. *How will clients authenticate to the SharePoint web application?*
   Select whether your SharePoint clients are using NTLM authentication, or smart card authentication.

   ▸ **Clients use smart card authentication**
   Select this option if your clients are using smart cards to authenticate to the SharePoint implementation.

   In this scenario, when a client attempts to access SharePoint, the BIG-IP system requests a certificate from the client. Because this certificate is stored on a smart card, the user must enter a PIN to authenticate to the smart card. The certificate must contain the user's account name in User Principal Name (UPN) format. The BIG-IP APM extracts the UPN from the certificate, extracts the user name and domain name from the UPN, and uses these credentials to obtain a Kerberos ticket from a domain controller in the user's Active Directory domain. Using this ticket, APM then authenticates to SharePoint on behalf of the client.

   i). *What is the Kerberos Key Distribution Center IP or FQDN?*
   Specify the IP address or FQDN of your Kerberos Key Distribution Center (KDC). The KDC is a network service that supplies session tickets and temporary session keys to users and computers within an AD domain.

If using an FQDN, this BIG-IP system must be able to resolve the IP address of the KDC using DNS.

ii). *What is the Active Directory Kerberos Realm the smart cards use?*
Specify the Kerberos Realm the used by the smart cards to authenticate. While this should be entered in all capital letters, the iApp automatically capitalizes any lower case letters when you submit the template.

iii). *What is the user name for the Active Directory delegation account you created?*
Specify the user name for the delegation account you created in your Active Directory implementation.

iv). *What is the associated password?*
Specify the password for the account you entered in the previous question.

- **Clients use NTLM authentication**
  Select this option if your SharePoint clients use NTLM to authenticate to the SharePoint implementation.

  i). *Should APM create a pool of Active Directory servers for authentication requests?*
  Select whether you want the BIG-IP APM to create a pool of multiple Active Directory servers, or to use a single Active Directory server to service authentication requests.

  We recommend using a pool of servers, which enables high availability and redundancy.

  - **No, use a single Active Directory server**
    Select this option if you want APM to use a single Active Directory server for authentication requests.

    1). *Which Active Directory server IP address in your domain can this BIG-IP system contact?*
    Specify the IP address of the Active Directory server you want the BIG-IP APM to use for servicing authentication requests.

  - **Yes, create a pool of Active Directory servers**
    Select this option have multiple Active Directory servers you want to use for implementation. The iApp creates a load balancing pool for the Active Directory servers you specify.

    1). *Which Active Directory servers in your domain can this BIG-IP system contact?*
    Specify both the FQDN and IP address of each Active Directory server you want the BIG-IP APM to use for servicing authentication requests. Click Add to include additional servers.

  ii). *What is the FQDN of your Active Directory domain for your SharePoint users?*
  Specify the FQDN of the Active Directory deployment for your SharePoint users. This is the FQDN for your domain, such as example.com, rather than the FQDN for any specific host.

  iii). *Does your Active Directory domain allow anonymous binding?*
  Select whether anonymous binding is allowed in your Active Directory environment.

  - **Yes, anonymous binding is allowed**
    Select this option if anonymous binding is allowed. No further information is required.

  - **No, credentials are required for binding**
    If credentials are required for binding, you must specify an Active Directory user name and password for use in the AAA Server.

    1). *Which Active Directory user with administrative permissions do you want to use?*
    Type a user name with administrative permissions.

    2). *What is the password associated with that account?*
    Type the associated password.

  iv). *How do you want to handle health monitoring for this pool?*
  Specify whether you want the template to create a new LDAP monitor or a new ICMP monitor, or if you select an existing monitor. For more accurate monitoring, we recommend using an LDAP monitor.

  - **Select an existing monitor for the Active Directory pool**
    Select this option if you have already created a health monitor (only monitors with a **Type** of LDAP or External can be used) for the Active Directory pool that will be created by the template. If you want to create a health monitor, but have not already done so, you must exit the template and create the object before it becomes available from the list.

    The iApp allows you to select monitors that are a part of another iApp Application Service. If you select a monitor that is a part of another Application Service, be aware that any changes you make to the monitor in the other Application Service will apply to this Application Service as well.

1). *Which monitor do you want to use?*
From the list, select the LDAP or External monitor you created to perform health checks for the Active Directory pool created by the template. Only monitors that have a Type value of LDAP or External appear in this list. Continue with the next section.

- **Use a simple ICMP monitor for the Active Directory pool**
Select this option if you only want a simple ICMP monitor for the Active Directory pool. This monitor sends a ping to the servers and marks the server UP if the ping is successful.
Continue with the next section.
- **Create a new LDAP monitor for the Active Directory pool**
Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

1). *Which Active Directory user name should the monitor use?*
Specify an Active Directory user name for the monitor to use when attempting to log on as a part of the health check. This should be a user account created specifically for this health monitor, and *must* be set to never expire.

2). *What is the associated password?*
Specify the password associated with the Active Directory user name.

3). *What is the LDAP tree for this user account?*
Specify the LDAP tree for the user account. As noted in the inline help, ADSI editor, an tool for Active Directory LDAP administration, is useful for determining the correct LDAP tree value. For example, if the user name is 'user1' which is in the organizational unit 'F5 Users' and is in the domain 'f5.example.com', the LDAP tree would be: ou=F5 Users, dc=f5, dc=example, dc=com.

4). *Does your Active Directory domain require a secure protocol for communication?*
Specify whether your Active Directory implementation requires SSL or TLS for communication, or does not require a secure protocol. This determines the port the health monitor uses.

* **No, a secure protocol is not required**
Select this option if your Active Directory domain does not require a secure protocol.

* **Yes, SSL communication is required**
Select this option if your Active Directory domain requires SSL communication. The health check uses port 636 as the Alias Service Port.

* **Yes, TLS communication is required**
Select this option if your Active Directory domain requires TLS communication. The health check uses port 389 as the Alias Service Port.

5). *How many seconds between Active Directory health checks?*
Specify how many seconds the system should use as the health check Interval for the Active Directory servers. We recommend the default of 10 seconds.

6). *Which port is used for Active Directory communication?*
Specify the port being used by your Active Directory deployment. The default port displayed here is determined by your answer to the secure protocol question. When using the TLS security protocol, or no security, the default port 389. The default port used when using the SSL security protocol is 636.

SSL Encryption

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 processing client-side SSL.

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. ***How should the BIG-IP system handle SSL traffic?***
There are four options for configuring the BIG-IP system for SSL traffic (only two are available if you deployed BIG-IP APM in the previous section. Select the appropriate mode for your configuration.

- **Encrypt to clients, plaintext to servers (SSL Offload)**
  Choose this method if you want the BIG-IP system to offload SSL processing from the servers. You need a valid SSL certificate and key for this method. Be sure to see *Appendix A: Configuring SharePoint Alternate Access Mappings to support SSL offload on page 42*.

  a. *Which Client SSL profile do you want to use?* **Advanced**
  Select whether you want the iApp to create a new Client SSL *profile*, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

  Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  - *Select an existing Client SSL profile*
    If you created a Client SSL profile for this implementation, select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.

  - Create a new Client SSL profile
    Select this option for the iApp to create a new Client SSL profile

    i). *Which SSL certificate do you want to use?*
    Select the SSL certificate you imported for this implementation.

    ii). *Which SSL private key do you want to use?*
    Select the associated SSL private key.

    iii). *Which intermediate certificate do you want to use?* **Advanced**
    If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

- **Terminate SSL from clients, re-encrypt to servers (SSL Bridging)**
  Choose this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers (SSL Bridging). You need a valid SSL certificate and key for the client-side, and optionally for the server-side (see #b).

  a. *Which Client SSL profile do you want to use?* **Advanced**
  Select whether you want the iApp to create a new Client SSL *profile*, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

  Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  - *Select an existing Client SSL profile*
    If you created a Client SSL profile for this implementation select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.

  - Create a new Client SSL profile
    Select this option for the iApp to create a new Client SSL profile

    i). *Which SSL certificate do you want to use?*
    Select the SSL certificate you imported for this implementation.

    ii). *Which SSL private key do you want to use?*
    Select the associated SSL private key.

    iii). *Which intermediate certificate do you want to use?* **Advanced**
    If your implementation requires an intermediate or chain certificate, select the appropriate certificate from the list.

Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

b. *Which Server SSL profile do you want to use?*
Select whether you want the iApp to create the F5 recommended Server SSL profile, or if you want to choose a Server SSL profile you already created. In this scenario, the BIG-IP system is acting as an SSL client and by default, we assume the servers do not expect the BIG-IP system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must create a custom Server SSL profile with the appropriate certificate and key.

The default, F5 recommended Server SSL profile uses the serverssl parent profile. For information about the ciphers used in the Server SSL profile, see *http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html*.

- **Encrypted traffic is forwarded without decryption (SSL pass-through)**
Choose this method if you do not want the BIG-IP system to do anything with encrypted traffic and simply send it to the SharePoint servers. This is similar to SSL bridging, although in this case the system does not decrypt then re-encrypt the traffic, it only sends it on to the servers without modification.

  If you select this option, the system defaults to Source Address Persistence for SharePoint 2010. Persistence is not recommended for SharePoint 2013.

- **Plaintext to clients, encrypt to servers**
Choose this method if you want the BIG-IP system to accept plain text from the clients and then encrypt it before sending it to the servers.

  Unless you have requirements for configuring specific Server SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Server** to create a Server SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  The default, F5 recommended Server SSL profile uses the *serverssl* parent profile. For information about the ciphers used in the Server SSL profile, see *http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html*.

- **Plaintext to both clients and servers**
Choose this method if the BIG-IP system is not sending or receiving any SSL traffic in this implementation.

Application Security Manager (BIG-IP ASM)

This section gathers information about BIG-IP Application Security Manager if you want to use it to protect the SharePoint deployment.

1. ***Do you want to deploy BIG-IP Application Security Manager?***
Choose whether you want to use BIG-IP ASM, F5's advanced application firewall, to secure this SharePoint deployment. If you choose to use BIG-IP ASM, the iApp template sets the policy enforcement mode to transparent. In this mode, violations are logged but not blocked. Before manually changing the enforcement mode to blocking, review the ASM log results and adjust the policy for your deployment if necessary. See the BIG-IP ASM documentation for specific details on configuring ASM.

- **Do not use Application Security Manager**
Select this option if you do not want to enable BIG-IP ASM at this time. You can always re-enter the template at a later date to enable BIG-IP ASM.

- **Use Application Security Manager**
Select this option if you want to enable BIG-IP ASM to protect your SharePoint implementation.

  a. *Which logging profile would you like to use?*
  Choose whether you or not you want to use a logging profile for this ASM implementation. You can configure the BIG-IP system to log detailed information about BIG-IP ASM events and store those logs on the BIG-IP system or a remote logging server (supports syslog and splunk). If you want to use a logging profile, we recommend creating one outside this template. The list only contains profiles with Application Security enabled.

- Do not apply a logging profile
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.

- *Select an existing logging profile from the list*
  If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging Profiles**. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the ***BIG-IP Network Firewall: Policies and Implementations*** guide for more information.

b. *Which language encoding is used for ASM?*
Select the language encoding for SharePoint. The language encoding determines how the security policy processes the character sets. The default language encoding determines the default character sets for headers, objects, parameter names, and parameter values.

Application Firewall Manager (BIG-IP AFM)

This section gathers information about BIG-IP Advanced Firewall Manager if you want to use it to protect the SharePoint deployment. For more information on configuring BIG-IP AFM, see *http://support.f5.com/kb/en-us/products/big-ip-afm.html*, and then select your version.

1. ***Do you want to use BIG-IP AFM to protect your application?***
Choose whether you want to use BIG-IP AFM, F5's network firewall, to secure this SharePoint deployment. If you choose to use BIG-IP AFM, you can restrict access to the SharePoint virtual server to a specific network or IP address. See the BIG-IP AFM documentation for specific details on configuring AFM.

- No, do not use Application Firewall Manager
  Select this option if you do not want to enable BIG-IP AFM at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.

- *Select an existing AFM policy from the list*
  If you already created a BIG-IP AFM policy for this implementation, select it from the list. Continue with ***c***.

- Yes, use F5's recommended AFM configuration
  Select this option if you want to enable BIG-IP AFM using F5's recommended configuration.

a. *Do you want to restrict access to your application by network or IP address?*
Choose whether you want to restrict access to the SharePoint implementation via the BIG-IP virtual server.

- No, do not restrict source addresses (allow all sources)
  By default, the iApp configures the AFM to accept traffic destined for the SharePoint virtual server from all sources. If you do not have a need to restrict access to the virtual server, leave this option selected and then continue with ***b***.

- Restrict source addresses
  Select this option if you want to restrict access to the SharePoint virtual server by IP address or network address.

i). *What IP or network addresses should be allowed to access your application?*
Specify the IP address or network access that should be allowed access to the SharePoint virtual server. You can specify a single IP address, a list of IP addresses separated by spaces (not commas or other punctuation), a range of IP addresses separated by a dash (for example **`192.0.2.10-192.0.2.100`**), or a single network address, such as **`192.0.2.200/24`**.

b. *How do you want to control access to your application from sources with a low reputation score?*
The BIG-IP AFM uses an IP intelligence database to categorize IP addresses coming into the system. Choose what you want the system to do for sources that are attempting to access the SharePoint virtual server with a low reputation score. For more information, see the BIG-IP AFM documentation.

Important: You must have an active IP Intelligence license for this feature to function. See *https://f5.com/products/modules/ip-intelligence-services for information*.

See page 41 of the troubleshooting section for a mandatory modification to the configuration if you are using AFM and the IP Intelligence feature to restrict or log traffic with low reputation scores.

- **Allow all sources regardless of reputation**
  Select this option to allow all sources, without taking into consideration the reputation score.
- **Reject access from sources with a low reputation**
  Select this option to reject access to the SharePoint virtual server from any source with a low reputation score.
- **Allow but log access from sources with a low reputation**
  Select this option to allow access to the SharePoint virtual server from sources with a low reputation score, but add an entry for it in the logs.

c. *Would you like to stage a policy for testing purposes?*
Choose whether you want to stage a firewall policy for testing purposes. A staged policy allows you to evaluate the effect a policy has on traffic by analyzing the system logs, without actually modifying traffic based on the firewall rules. You must already have a policy on the system in order to select it.

- **Do not apply a staging policy**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing policy from the list*
  If you have already created a firewall policy for this implementation, select it from the list. Only policies that already exist on the system appear in the list. To create a new policy, on the Main tab, click **Security > Network Firewall > Policies**. Specific instructions for creating a firewall policy is outside the scope of this iApp and deployment guide.

d. *Which logging profile would you like to use?*
Choose whether you or not you want to use a logging profile for this AFM implementation. You can configure the BIG-IP system to log detailed information about BIG-IP system Network Firewall events and store those logs on the BIG-IP system or a remote logging server (supports syslog and Splunk). If you want to use a logging profile, we recommend creating one outside this template. The list only contains profiles with Network Firewall enabled.

- **Do not apply a logging profile**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing logging profile from the list*
  If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging Profiles**. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the ***BIG-IP Network Firewall: Policies and Implementations*** guide for more information.

Virtual Server and Pools

This section gathers information about your SharePoint deployment that will be used in the BIG-IP *virtual server* and *load balancing pool*.

1. ***What IP address do you want to use for the virtual server?***
   Type the IP address you want to use for the BIG-IP virtual server. This is the address clients use (or a DNS entry resolves to this address) to access the SharePoint deployment via the BIG-IP system.

   If necessary for your configuration, this can be a network address to create a network virtual server (you must specify an IP mask in the following question for a network virtual server). A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0), allowing the BIG-IP system to direct client connections that are destined for an entire range of IP addresses, rather than for a single destination IP address. Thus, when any client connection targets a destination IP address that is in the network specified by the virtual server IP address, the system can direct that connection the pool of SharePoint servers.

2. ***If using a network virtual address, what is the IP mask?*** Advanced
   If you specified a network address for the virtual server (allowing the virtual server to handle multiple IP addresses), you must enter the full network mask representing the address range. If you specified a single address for the virtual server, you may leave this field blank.

3. ***What port do you want to use for the virtual server?***
   Type the port number you want to use for the BIG-IP virtual server. For SharePoint deployments, this is typically 80 (HTTP) or 443 (HTTPS). The default port in the box is based on your answer to the How should the system handle SSL traffic question.

4. ***Which FQDNs will clients use to access the servers?***
   Type each fully qualified domain name clients will use to access the SharePoint deployment. Click the **Add** button to insert additional rows. If you only have one FQDN, do not click Add.

   If you are also deploying the BIG-IP system for SharePoint Apps in SharePoint 2013, or if you have Office Web Apps accessed through the SharePoint virtual server, you must also add those FQDN(s).

5. ***Do you want to redirect inbound HTTP traffic to HTTPS?*** Advanced
   This question only appears if you selected SSL Offload or SSL Bridging in the SSL question.

   Select whether you want the BIG-IP system to automatically redirect HTTP traffic to the HTTPS virtual server. This is useful when users forget to use HTTPS when attempting to connect to the Microsoft SharePoint deployment.

   - **Redirect HTTP to HTTPS**
     Select this option to redirect HTTP traffic to HTTPS. If you select this option (the default), the BIG-IP system attaches a very small redirect iRule to the virtual server.

     a. *From which port should traffic be redirected?*
        Type the port number for the traffic that you want to redirect to HTTPS. The most common is port 80 (the default).

   - **Do not redirect HTTP to HTTPS**
     Select this option if you do not want to enable the automatic redirect.

6. ***Which HTTP profile do you want to use?*** Advanced
   The HTTP *profile* contains settings for instructing the BIG-IP system how to handle HTTP traffic. Choose whether you want the iApp to create a new HTTP profile or if you have previously created an HTTP profile for this deployment.

   Unless you have requirements for configuring specific HTTP settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP** to create a HTTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select an existing HTTP profile from the list*
     If you already created an HTTP profile for this implementation, select it from the list.

   - **Create a new HTTP profile (recommended)**
     Select this option for the iApp to create a new HTTP profile.

     a. *Should the BIG-IP system insert the X-Forwarded-For header?* Advanced
        Select whether you want the BIG-IP system to insert the X-Forwarded-For header in the HTTP header for logging purposes.

        - **Insert the X-Forwarded-For header**
          Select this option if you want the system to include the X-Forwarded-For header. You may have to perform additional configuration on your SharePoint servers to log the value of this header. For more information on configuring logging see *Appendix D: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 57*.

        - **Do not insert the X-Forwarded-For header**
          Select this option if you do not want the system to include X-Forwarded-For in the HTTP header.

7. ***Which persistence profile do you want to use?*** Advanced
   By using persistence, the BIG-IP system tracks and stores session data, such as the specific pool member that serviced a client request, ensuring client requests are directed to the same pool member throughout the life of a session or during subsequent sessions. If you are using SharePoint 2013, the default is Do not use persistence.

   Unless you have requirements for configuring specific persistence settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Persistence** to create a persistence profile.

To select any new profiles you create, you need to restart or reconfigure this template. Select one of the following persistence options:

- **Use Cookie Persistence**
  This is the recommended option if you are using SharePoint 2010 and not using SSL pass-through.
  Leave this option to have the BIG-IP system create a new cookie persistence profile (cookie insert mode). With Cookie persistence, the BIG-IP system uses an HTTP cookie stored on the client's computer to allow the client to reconnect to the same server previously visited.

- **Source IP Address persistence**
  This is the recommended option if you are using SharePoint 2010 and selected SSL pass-through.
  Select this option if you want to use the Source IP address (also known as simple) persistence. With this mode, the BIG-IP system assigns the built-in Source Address Affinity persistence type, and directs session requests to the same server based only on the source IP address.

- **Do not use persistence**
  This is the recommended option if you are using SharePoint 2013.
  If your implementation does not require persistent connections, select this option. SharePoint 2013 does not require connections from a single client to persist to the same SharePoint server, as the Distributed Cache service maintains authentication information across all SharePoint web application servers.

- *Select an existing persistence profile*
  If you have previously created a persistence profile, you have the option of selecting it instead of allowing the iApp to create a new one. From the list, select an existing persistence profile. We recommend using a persistence profile that uses Cookie persistence, Insert mode.

8. ***Do you want to create a new pool or use an existing one?***
   A *load balancing pool* is a logical set of servers, grouped together to receive and process traffic. When clients attempt to access the application via the BIG-IP virtual server, the BIG-IP system distributes requests to any of the servers that are members of that pool.

   - *Select an existing pool*
     If you have already created a pool for your SharePoint servers, you can select it from the list.
     If you do select an existing pool, all of the rest of the questions in this section disappear.

   - **Do not use a pool**
     If you are deploying this iApp in such a way that you do not need a pool of SharePoint servers, select this option. If you specified that the servers are connected to the BIG-IP system over the WAN through another BIG-IP system, this is the default option, as the system is sending the traffic across the iSession tunnel to the other BIG-IP system to be distributed to the servers.

   - **Create a new pool**
     Leave this default option to create a new load balancing pool and configure specific options.

     a. *Which load balancing method do you want to use?* Advanced
        Specify the load balancing method you want to use for this SharePoint server pool. We recommend the default, **Least Connections (member)**.

     b. *Do you want to give priority to specific groups of servers?* Advanced
        Select whether you want to use Priority Group Activation. Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP then sends traffic to the group of servers with the next highest priority, and so on. See the BIG-IP documentation for more details.

        - **Do not use Priority Group Activation (recommended)**
          Select this option if you do not want to enable Priority Group Activation.

        - **Use Priority Group Activation**
          Select this option if you want to enable Priority Group Activation.
          You must add a priority to each server in the Priority box described in #c.

i). What is the minimum number of active members for each priority group?
Specify the minimum number of servers that must be active to continue sending traffic to the priority group. If the number of active servers falls below this minimum, traffic will be sent to the group of servers with the next highest priority group number.

c. *Which SharePoint servers should be included in this pool?*
Specify the IP address(es) of your SharePoint servers. If you have existing nodes on this BIG-IP system, you can select them from the list, otherwise type the addresses. You can optionally add a Connection Limit. If you enabled Priority Group Activation, you must also specify a Priority for each device. Click **Add** to include additional servers.

Delivery Optimization

In this section, you answer questions about how you want the BIG-IP system to optimize the delivery of your SharePoint traffic.

1. ***Use the BIG-IP Application Acceleration Manager?***
Choose whether you want to use the BIG-IP Application Acceleration Manager (formerly known as WebAccelerator). BIG-IP Application Acceleration Manager helps accelerate your SharePoint traffic.

▶ **Yes, use BIG-IP AAM (recommended)**
Select this option to enable BIG-IP AAM.

▶ **No, do not use BIG-IP AAM**
Select this option if you do not want to enable BIG-IP AAM at this time.

2. ***Which Web Acceleration profile do you want to use for caching?*** **Advanced**
Select whether you want the system to create a new Web Acceleration profile, or if you have already created a Web Acceleration profile for use in this deployment. The Web Acceleration profile contains the caching settings for this implementation.

Unless you have requirements for configuring specific acceleration settings (such as specific allowing/denying specific URIs), we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : Web Acceleration** to create an acceleration profile. To select any new profiles you create, you need to restart or reconfigure this template.

Note if using BIG-IP AAM:
If you are using BIG-IP AAM, and want to select a custom Web Acceleration profile for caching you have already created, it must have an AAM application enabled, otherwise it does not appear in the list of caching profiles. If you want access to all Web Acceleration profiles on the box, then you must choose No to the use BIG-IP AAM question. Use a custom Web Acceleration profile only if you need to define specific URIs that should or should not be cached.

Note if not using BIG-IP AAM:
If you are not using BIG-IP AAM, we recommend you only use a custom Web Acceleration profile if you need to define specific URIs which should or should not be cached.

▶ **Create a profile based on optimized-caching (recommended)**
Leave this default option to create a new Web Acceleration profile for caching.

▶ **Do not use caching**
This question does not appear if you chose to enable BIG-IP AAM
Select this option if you do not want to enable caching on the BIG-IP system for this implementation.

▶ *Select an existing Web Acceleration profile*
If you have already created a Web Acceleration profile for your SharePoint servers, you can select it from the list.

3. ***Do you want to insert the X-WA-Info header?*** **Advanced**
This question only appears if you chose to enable BIG-IP AAM

The BIG-IP system can optionally insert an X-WA-Info response header that includes specific codes describing the properties and history of the object. The X-WA-Info response header is for informational and debugging purposes only and provides a way for you to assess the effectiveness of your acceleration policy rules.

By default, the AAM X-WA-info header is not included in the response from the BIG-IP system. If you choose to enable this header, you have two options, Standard and Debug. In Standard mode, the BIG-IP system inserts an HTTP header that includes numeric codes which indicate if and how each object was cached. In Debug mode, the BIG-IP system includes additional information which may help for extended troubleshooting.

- **Do not insert the header (recommended)**
  Select this option if you do not want to insert the X-WA-Info header. Typically F5 recommends not inserting the header unless instructed to do so by an F5 Technical Support Engineer.
- **Insert the Standard header**
  Select this option if you want to insert the Standard header. For detailed information on the numeric codes used by the header, see *http://support.f5.com/kb/en-us/solutions/public/13000/700/sol13798.html*
- **Insert the Debug header**
  Select this option if you want to insert the Debug header for extended troubleshooting.

4. ***Do you want to use the legacy AAM performance monitor?*** Advanced
   This question only appears if you chose to enable BIG-IP AAM

   Enabling the legacy AAM performance monitor can adversely affect system performance. This monitor is primarily used for legacy AAM performance monitoring and debugging purposes, and can adversely affect system performance. The BIG-IP Dashboard provides performance graphs and statistics related to AAM.

   - **Do not enable the legacy performance monitor (recommended)**
     Select this option if you do not want to enable the legacy monitor.
   - **Enable the legacy performance monitor**
     Select this option if you want to enable the legacy performance monitor. Remember enabling this legacy monitor can impact overall system performance.

     a. *For how many days should the BIG-IP system retain the data?*
        Specify the number of days the BIG-IP system should retain the legacy performance data.

5. ***Which acceleration policy do you want to use?*** Advanced
   This question only appears if you chose to enable BIG-IP AAM

   Unless you have created a custom BIG-IP AAM policy for this deployment, select the default policy (**Microsoft SharePoint 2010**). This predefined acceleration policy was created for Microsoft SharePoint servers.

6. ***Which compression profile do you want to use?***
   Compression improves performance and end user experience for Web applications that suffer from WAN latency and throughput bottlenecks. Compression reduces the amount of traffic sent to the client to complete a transaction.

   Unless you have requirements for configuring specific compression settings, we recommend allowing the iApp to create a new profile. F5 recommends the default profile which is optimized for SharePoint servers. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP Compression** to create a compression profile. To select any new profiles you create, you need to restart or reconfigure this template.

7. ***How do you want to optimize client-side connections?*** Advanced
   The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create the appropriate tcp-optimized profile (recommended)**
     Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects clients to the BIG-IP system" question.

- *Select the TCP profile you created from the list*
  If you created a custom TCP profile for the SharePoint servers, select it from the list.

Server offload

In this section, you configure the options for offloading tasks from the SharePoint servers. This entire section only appears if you selected Advanced mode.

1. ***Which OneConnect profile do you want to use?*** Advanced
   OneConnect (connection pooling or multiplexing) improves server scalability by reducing load associated with concurrent connections and connection rate to SharePoint servers. When enabled, the BIG-IP system maintains one connection to each SharePoint server which is used to send requests from multiple clients.

   Unless you have requirements for configuring specific settings, we recommend allowing the iApp to create a new profile. F5 recommends the default profile which is optimized for SharePoint servers. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Other : OneConnect** to create a OneConnect profile. To select any new profiles you create, you need to restart or reconfigure this template.

   If you are deploying SharePoint 2013, and want to select a custom OneConnect profile, be sure it has a 0.0.0.0 source mask.

   - **Create a profile based on the oneconnect parent (recommended)**
     Select this option to have the system create the recommended OneConnect profile. The system uses the oneconnect parent profile with a Source Mask setting of 255.255.255.255.
   - **Do not use a OneConnect profile**
     Select this option if you do not require the BIG-IP system to perform connection pooling using a OneConnect profile.
   - *Select the OneConnect profile you created from the list*
     If you created a custom OneConnect profile for the SharePoint servers, select it from the list.

2. ***Which NTLM profile do you want to use?*** Advanced
   The NTLM profile optimizes network performance when the system is processing NTLM traffic. When both an NTLM profile and a OneConnect profile are enabled, the system can take advantage of server-side connection pooling for NTLM connections.

   If you are creating this template in a BIG-IP partition other than /Common, you must create a custom NTLM profile and select it from this list. See *Troubleshooting on page 38* for detailed information.

   If your environment uses NTLM, we recommend allowing the iApp to create a new profile unless you have requirements for configuring specific settings. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Other : NTLM** to create a NTLM profile. To select any new profiles you create, you need to restart or reconfigure this template.

   If you are deploying SharePoint 2013, select **Do not use NTLM (recommended)**.

   - **Use F5's recommended NTLM profile**
     Select this option to have the system create the recommended NTLM profile. The system uses the ntlm parent profile.
   - **Do not use NTLM (recommended)**
     Select this option if you do not use NTLM authentication in your SharePoint implementation.
   - *Select the NTLM profile you created from the list*
     If you created a custom NTLM profile for the SharePoint servers, select it from the list.

3. ***How do you want to optimize server-side connections?*** Advanced
   The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Create the appropriate tcp-optimized profile (recommended)**
  Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects servers to the BIG-IP system" question.
- *Select the TCP profile you created from the list*
  If you created a custom TCP profile for the SharePoint servers, select it from the list.

4. ***Do you want the BIG-IP system to queue TCP requests?***
Select whether you want the BIG-IP system to queue TCP requests. 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 according to defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on AskF5.

ⓘ ***Important***

TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance.
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 nodes.

- **No, do not enable TCP request queuing (recommended)**
  Select this option if you do not want the BIG-IP system to queue TCP requests.
- **Yes, enable TCP request queuing**
  Select this option if you want to enable TCP request queuing on the BIG-IP system.
  a. *What is the maximum number of TCP requests for the queue?*
  Type the maximum number of requests you want to queue. We do ***not*** recommend using 0, which means unlimited and is only constrained by available memory.
  b. *How many milliseconds should requests remain in the queue?*
  Type a number of milliseconds for the TCP request timeout value.

5. ***Use a Slow Ramp time for newly added servers?*** Advanced
With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added SharePoint server over a time period you specify, rather than sending a full proportion of the traffic immediately. Slow Ramp is essential when using the Least Connections load balancing method (our recommended method for SharePoint servers), as the BIG-IP system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

Select whether you want to use a Slow Ramp time.

- **Use Slow Ramp**
  Select this option for the system to implement Slow Ramp time for this pool.
  a. *How many seconds should Slow Ramp time last?*
  Specify a duration in seconds, for Slow Ramp. The time period you select for Slow Ramp is highly dependent on the speed of your server hardware and the behavior of your web services. The default setting of 300 seconds (5 minutes) is very conservative in most cases.
- **Do not use Slow Ramp**
  Select this option if you do not want to use Slow Ramp. If you select this option, we recommend you do not use the Least Connections load balancing method.

Application Health

In this section, you answer questions about how you want to implement application health monitoring on the BIG-IP system.

1. ***Create a new health monitor or use an existing one?***
   Application health monitors are used to verify the content that is returned by an HTTP request. The system uses these monitors to ensure traffic is only sent to available SharePoint servers.

   Unless you have requirements for configuring other options not in the following list of questions, we recommend allowing the iApp to create a new monitor. Creating a custom health monitor is not a part of this template; see **Local Traffic** >> **Monitors**. To select any new monitors you create, you need to restart or reconfigure this template.

   If you configured your SharePoint web application to use AD FS as a Trusted Identity authentication provider, see *Optional: Monitoring SharePoint Web Applications Configured for AD FS as a Trusted Identity Provider on page 30.*

   - *Select the monitor you created from the list*
     If you manually created the health monitor, select it from the list.
     Continue with *iRules on page 29.*

   - Create a new health monitor
     If you want the iApp to create a new monitor, continue with the following.

     a. *How many seconds should pass between health checks?*
     Specify how long the system should wait between each health check. This is used as the Interval setting for the monitor. We recommend the default of 30 seconds.

     b. *What type of HTTP request should be sent to the servers?*
     Select whether you want the system to send an HTTP GET or POST request. The GET method requests data from the server, the POST submits data to be processed by the server.

     - GET
       Select this option if you want the system to use a GET request. The system uses the URI you specify in the next question to request content from the SharePoint server.

     - POST
       Select this option if you want the system to use a POST request. The system uses the URI you specify in the next question, along with the HTTP POST body you will specify to form the request.

     c. *What HTTP URI should be sent to the servers?*
     The HTTP URI is used to specify the resource on the SharePoint server for a given request. This parameter can be customized to request a specific part of your application, which can indicate the application-health on a granular level.

     d. *What HTTP version do your servers expect clients to use?*
     Choose the HTTP version which you expect most of your clients to be using. This allows the system to detect failures more accurately.

     - HTTP/1.0
       Choose this option if you expect your clients to use HTTP/1.0.

     - HTTP/1.1
       Choose this option if you expect your clients to use HTTP/1.1.

     e. *What HTTP POST body do you want to use for this monitor?*
     This question only appears if you selected a POST request.

     If you selected a POST request, you must specify the message body for the POST.

     f. *What is the expected response to the HTTP request?*
     Specify the response you expect returned from the request. The system checks the response from the server against the response you enter here to determine server health.

     g. *Should the health monitor require credentials?*
     Choose whether you want the system to attempt to authenticate to the SharePoint deployment as a part of the health check.

     - No, allow anonymous access
       Select this option if you do not want the monitor to attempt authentication.

- **Yes, require credentials for Basic authentication**
  Select this option if you want to attempt Basic authentication as a part of the health monitor. To require credentials, you should have a user account specifically for this health monitor which has no other privileges, and has a password set to never expire.

  i). *What user name should the monitor use?*
  Type the domain and user name for the account you created for the health monitor. You must include the domain in front of the user, such as EXAMPLE\USER.

  ii). *What is the associated password?*
  Type the password for the account.

- **Yes, require credentials for NTLM authentication**
  Select this option if you want to attempt NTLM authentication as a part of the health monitor. To require credentials, you should have a user account specifically for this health monitor which has no other privileges, and has a password set to never expire.

  i). *What user name should the monitor use?*
  Type the user name for the account you created for the health monitor.

  ⚠ ***Warning***

  Do not include DOMAIN\ for the NTLM monitor user name.

  ii). *What is the associated password?*
  Type the password for the account.

iRules

In this section, you can add custom iRules to the SharePoint deployment. This section is available only if you selected Advanced mode. iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to the configuration?*** **Advanced**
   Select if have preexisting iRules you want to add to your SharePoint implementation.

   ⚠ ***Warning***

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates for your SharePoint servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Statistics and Logging

In this section, you answer questions about logging and statistics settings. This section is available only if you selected Advanced mode.

1. ***Do you want to enable Analytics for application statistics?***
   The Application Visibility Reporting (AVR) module for analytics allows you to view statistics specific to your application implementation. AVR is included and available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that this provisioning requirement is only for AVR, you can view object-level statistics from the BIG-IP system without provisioning AVR.

   ⓘ ***Important***

   Enabling Analytics may adversely affect overall system performance. If you choose to enable Analytics, we recommend gathering statistics for a set time period, such as one week, and then re-entering this template and disabling Analytics while you process the data.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile. 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. To select the new profile, you need to restart or reconfigure the iApp template.

- **Do not enable Application Visibility Reporting**
  If you do not want to enable Analytics, leave this list set to **No**, and continue with the next section.
- *Select the Analytics profile you created from the list*
  If you choose to enable Analytics, select the Analytics profile you want to use for this implementation from the list.

2. ***Which HTTP request logging profile do you want to use?***
   HTTP request logging enables customizable log messages to be sent to a syslog server for each HTTP request processed by your application. You can choose to enable HTTP request logging by selecting a logging profile you already created from the list.
   We strongly recommend you thoroughly test the performance impact of using this feature in a staging environment prior to enabling on a production deployment

   Creating a request logging profile is not a part of this template. See Local Traffic>>Profiles: Other: Request Logging. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Do not enable HTTP request logging**
     If you do not want to enable HTTP request logging, leave this list set to **No**, and continue with the next section.
   - *Select the HTTP request logging profile you created from the list*
     If you choose to enable HTTP request logging, select the profile you want to use for this implementation from the list.

Finished

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

Optional: Monitoring SharePoint Web Applications Configured for AD FS as a Trusted Identity Provider

If you have configured your SharePoint web application to use AD FS as a Trusted Identity authentication provider, you must use a monitor that determines availability of SharePoint services without authenticating. You can create a new monitor with the iApp using the values indicated below for expected response and credentials, or you can manually create a custom monitor and assign it to the deployment using the iApp.

If you want to configure the monitor while running through the iApp template, use the following guidance:

- In the Application Health area, from the *Create a new health monitor or use an existing one?* question, select **Create a new health monitor**.
- From the *What is the expected response to the HTTP request?* question, type **X-MSDAVEXT**.
- From the *Should the health monitor require credentials?* question, select **No, allow anonymous access**.

f you want to configure the monitor manually, use the guidance for the HTTP health monitor found in *Appendix B: Manual configuration tables on page 45*, making sure to use **X-MSDAVEXT** as the Receive String. Then use the Reconfigure feature on the application service to re-enter the template, and then from the *Create a new health monitor or use an existing one?* question, select the monitor you created.

Modifying the iApp configuration

This section contains modifications to the iApp template that are mandatory in certain situations. Review the entries to see if these changes apply to your configuration.

Modifying the iApp configuration for SharePoint 2013 "Apps" if you deployed the iApp for SSL offload

SSL offload is not currently supported for SharePoint Apps. You must use the following procedures to support SharePoint Apps if you configured the BIG-IP system for offloading SSL. This allows you to offload SSL from the main SharePoint deployment, but still support SharePoint Apps with the BIG-IP system.

Creating a new health monitor and pool for the SharePoint servers

Use the following table for guidance on configuring the BIG-IP LTM for unencrypted connections to the SharePoint servers. For specific instructions on configuring these objects, see the online help or the BIG-IP documentation.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**http**
	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 Time	**300**
	Load Balancing Method	**Least Connections (Member)**
	Address	Type the IP Address of a SharePoint
	Service Port	**80** Click **Add** to repeat Address and Service Port for all nodes

Creating the iRule

The next task is to create the iRule. This iRule disables server side SSL (re-encryption) for all connections except SharePoint Apps. In the iRule, *apps.example.com* corresponds to the new base domain for SharePoint Apps that you configured in SharePoint Central Administration. For instructions on configuring SharePoint Central Administration, see the Microsoft documentation.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this iRule.
4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers. *You must replace the text in red with the appropriate values from your configuration.*

```
when HTTP_REQUEST {
   if {[HTTP::host] contains "apps.example.com"} {
      pool sharepoint_https_pool
   } else {
      SSL::disable serverside

      # uncomment all remaining lines if clients will be connecting to Office Web
      # Apps through this virtual server

      #if {[HTTP::host] contains "wac.example.com"} {
         #pool office_web_apps_pool
      #} else {
         pool sharepoint_http_pool
         persist none
      #}
   }
}
```

5. Click **Finished**.

Modifying the template configuration for SSL bridging mode and adding the virtual server

In this procedure, we modify the iApp configuration for SSL Bridging and to include the iRule you created.

To configure the BIG-IP system for SSL Bridging

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. In the SSL Encryption section, from the **How should the BIG-IP system handle SSL traffic?** question, select **Terminate SSL from clients, re-encrypt to servers (SSL Bridging)**.
5. Configure the SSL Bridging options that appear as applicable for your deployment. See *SSL Encryption on page 17* for details.
6. In the iRules section, from the **Do you want to add any custom iRules to this configuration?** question, select the iRule you just created and then click the Add (**<<**) button to move it to the selected list.
7. Click the **Finished** button.

This completes the Apps for SharePoint configuration.

Modifying the iApp configuration if you configured the iApp to create a new LDAP monitor for the AD pool

If you configured the iApp template to use BIG-IP APM, selected that APM should create a pool of Active Directory Servers, and selected a new LDAP monitor for the Active Directory pool, you must manually modify the User Name field in the monitor to use the full Active Directory common name. This is only necessary if all of the conditions are met.

To resolve this issue, you have two options. Create a new monitor and select it using the iApp template, or modify the existing monitor to correct the user name (requires disabling Strict Updates).

Creating a new monitor

If you do not want to disable the Strict Updates feature, you can create a new, custom LDAP monitor and then select it from the iApp template. To create the monitor, go to **Main tab > Local Traffic > Monitors > Create**. Select LDAP as the parent, and then enter all of the relevant information. Make sure to use the full Active Directory common name in the user name field. After clicking Finished, use the Reconfigure feature on the Application Service to re-enter the template and then select the new monitor from the iApp template.

Modifying the existing monitor

If you do not want to create a new monitor, you can modify the existing configuration produced by the iApp. This requires first disabling the Strict Updates feature.

To disable Strict Updates

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**.

To modify the LDAP monitor

1. On the Main tab, expand Local Traffic and then click Monitors.
2. From the list, click the LDAP monitor created by the template.
3. In the User Name field, type the full Active Directory common name.
4. Click **Update**.

Configuring a local virtual server for SharePoint (optional)

If you are not using split DNS, and requests from the SharePoint 2010 front end servers to the SharePoint URL are routed through the external SharePoint virtual server on the BIG-IP LTM you may see problems with missing page images, or issues loading or clicking the SharePoint ribbon when a request from the WFE server is load balanced to another server rather than to itself.

In this case, you need to configure a virtual server on the same local VLAN as the SharePoint 2010 servers that includes an iRule. The iRule ensures each request is directed to the same server that made it. You must also add a host entry to the WFE servers directing all requests for the SharePoint URL to the IP address of the internal SharePoint virtual server. See the Microsoft documentation for instructions.

This also applies to a SharePoint 2013 configuration if you are using BIG-IP APM.

Use the following table to create the objects on the BIG-IP LTM. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors *(Main tab-->Local Traffic-->Monitors)*	***Name***	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pools *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name	
	Health Monitor	Select the HTTP monitor you created above	
	Load Balancing Method	**Round Robin**	
	Address	Type the IP Address of your SharePoint server	
	Service Port	**80** Click **Add** to repeat Address and Service Port for all nodes	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***Persistence*** *(Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
iRules *(Main tab-->Local Traffic -->iRules)*	***Name***	Type a unique name	
	Definition	See the following section for the iRule definition	
Virtual Servers *(Main tab-->Local Traffic -->Virtual Servers)*	***Name***	Type a unique name.	
	Destination Address	Type the IP address for this virtual server	
	Service Port	**80**	
	Protocol Profile (Client)	Select the TCP LAN profile you created above	
	SNAT Pool	**Automap**	
	iRule	Enable the iRule you created above	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the persistence profile you created above	

Creating the iRule definition

Use the following for the Definition of the iRule, omitting the line numbers, and ***changing the red text to the name your pool***.

```
when CLIENT_ACCEPTED {
     set pm_selected 0
     foreach { pm } [members -list internal-SharePoint-pool-name] {
     if { $pm equals “[IP::remote_addr] 80” } {
          set pm_selected 1
          pool internal-SharePoint-pool-name member [IP::remote_addr]
     }
}
if { $pm_selected equals 0 } {
     pool internal-SharePoint-pool-name
     }
}
```

This completes the local virtual server configuration.

Supporting Host-Named Site Collections in SharePoint Server 2010 and 2013 (optional)

Microsoft SharePoint Server 2010 and 2013 support the deployment of multiple, host name-based site collections on a single web application. If you are using multiple, host name-based collections on a single application, and configured (or are configuring) the iApp template for SSL offload, you must use the following guidance to create a new HTTP profile and health monitor and attach them to the implementation using the iApp.

Use the following table to create the new objects. Settings not mentioned in the table can be configured as appropriate for your implementation.

BIG-IP LTM Object	Non-default settings/Notes	
HTTP Profile *(Main tab > Local Traffic > Profiles > Services > HTTP)*	***Name***	Type a unique name
	Request Header Insert	**FRONT-END-HTTPS: ON**
	Redirect Rewrite	**Matching**
	Insert X-Forwarded-For	**Enabled** (optional)
Health Monitors *(Main tab-->Local Traffic-->Monitors)*	***Name***	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String	If using NTLM Authentication: **GET /SitePages/Home.aspx HTTP/1.1\r\nHost: sharepoint.example.com\r\nFront-End-Https: On\r\n** If using Basic or Anonymous authentication **GET /SitePages/Home.aspx HTTP/1.1\r\nHost: sharepoint.example.com\r\nFront-End-Https: On\r\nConnection: Close\r\n\r\n**

The next task is to re-enter the template and configure the iApp to use the profile and health monitor you just created.

1. Re-enter the iApp template (on the Main tab, click **iApp** > **Application Services** > [name of your SharePoint application service] and then from the Menu bar, click **Reconfigure**).
2. From the "Which configuration mode do you want to use?" question, select **Advanced** (if necessary).
3. In the *Virtual Server and Pools* section, from the "Which HTTP profile do you want to use?" question, select the profile you just created.
4. In the *Application Health* section, from the "Create a new health monitor or use an existing one?" question, select the monitor you just created.
5. Click **Update**.

You should not configure Alternate Access Mappings for the SharePoint web application as detailed in Appendix A of this guide, because it is applicable to path-based site collections only. Instead, you must configure each SharePoint site collection URL to use **https://**. This must be done using the SharePoint Management Shell. For more information, consult the Microsoft documentation: *http://technet.microsoft.com/en-us/library/cc424952.aspx*.

F5's APM and AAM modules also support the deployment of host-named site collections. When deploying the SharePoint iApp, you must enter each site collection FQDN in the "What FQDNs will clients use to access the servers?" question of the template. When accessing the web application via BIG-IP APM, the client will be redirected to the primary authentication URI, which is the first host entered in the FQDNs table. After authentication, BIG-IP APM redirects the client to the original request URI.

Modifying the HTTP compression profile if using a previous version of the template

Important: This issue has been fixed in version 1.1.0 of the iApp template. If you are using a previous version of the template, we strongly recommend upgrading to version 1.1 (see *Upgrading an Application Service from previous version of the iApp template on page 10)*. If you cannot upgrade, use the following guidance.

F5 has discovered that the HTTP compression profile produced by the iApp contains an improperly formatted Content Include string, and the omission of this string can lead to poor application performance or unusually high memory consumption on the BIG-IP system.

Until the next revision of the iApp template, you must manually create a new HTTP Compression profile and attach it to the virtual server using the iApp.

<table>
<tr><th>BIG-IP LTM Object</th><th colspan="2">Non-default settings/Notes</th></tr>
<tr><td rowspan="5"><b><i>HTTP Compression</i></b>
<i>(Local Traffic > Profiles > Services)</i></td><td>Name</td><td>Type a unique name</td></tr>
<tr><td>Parent Profile</td><td><b>wan-optimized-compression</b></td></tr>
<tr><td rowspan="3">Content List--> Include List <i>(Copy and paste each entry to the <b>Content Type</b> box and click <b>Include</b>.)</i></td><td>text/(css|html|javascript|json|plain|postscript|richtext|rtf|vnd\.wap\.wml|vnd\.wap\.wmlscript|wap|wml|x-component|x-vcalendar|x-vcard|xml)</td></tr>
<tr><td>application/(css|css-stylesheet|doc|excel|javascript|json|lotus123|mdb|mpp|ms-excel|ms-powerpoint|ms-word|msaccess|msexcel|mspowerpoint|msproject|msword|photoshop|postscript|powerpoint|ps|psd|quarkexpress|rtf|txt|visio|vnd\.excel|vnd.\ms-access|vnd\.ms-excel|vnd\.ms-powerpoint|vnd\.ms-pps|vnd\.ms-project|vnd\.ms-word|vnd\.ms-works|vnd\.ms-works-db|vnd\.msaccess|vnd\.msexcel|vnd\.mspowerpoint|vnd\.msword|vnd\.powerpoint|vnd\.visio|vnd\.wap\.cmlscriptc|vnd\.wap\.wmlc|vnd\.wap\.xhtml\+xml|vnd\.word|vsd|winword|wks|word|x-excel|x-java-jnlp-file|x-javascript|x-json|x-lotus123|x-mdb|x-ms-excel|x-ms-project|x-mscardfile|x-msclip|x-msexcel|x-mspowerpoint|x-msproject|x-msword|x-msworks-db|x-msworks-wps|x-photoshop|x-postscript|x-powerpoint|x-ps|x-quark-express|x-rtf|x-vermeer-rpc|x-visio|x-vsd|x-wks|x-word|x-xls|x-xml|xhtml+xml|xls|xml)</td></tr>
<tr><td>image/(photoshop|psd|x-photoshop|x-vsd)</td></tr>
</table>

Adding the profile to the virtual server

The final task is to add the profile to the iApp configuration. If you manually configured the system, simply attach the profile to the virtual server. If you used the iApp, use the following procedure.

To add the iRule to the SharePoint virtual server

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. In the Delivery Optimization section, from the **Which compression profile do you want to use?** question, select the profile you just created.
5. Click the **Finished** button.

Configuring BIG-IP LTM/APM to support NTLMv2-only deployments (optional)

If you have configured your Microsoft Windows domain to support only NTLMv2 authentication and refuse LM/NTLM requests, you must either modify the configuration produced by the template by disabling the Strict Updates feature and add/modify the required objects for NTLMv2 authentication.

Disabling the strict updates feature on the iApp deployment

First you must 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**.

Creating a new NTLM SSO Configuration object

Next, you create a new NTLM SSO Configuration object on the BIG-IP APM.

1. On the Main tab, click **Access Policy > Access Profiles > SSO Configurations > NTLMv2**.
2. Click **Create**.
3. In the **Name** box, type a unique name.
4. In the NTLM Domain field, type the fully qualified name of the domain where users authenticate.
5. Click **Finished**.

Modifying the Access Profile

The final task is to update the Access Profile created by the iApp template to use the NTLM SSO Configuration object you just created.

1. On the Main tab, click **Access Policy > Access Profiles**.
2. Click the name of the Access Profile created by the template. This profile starts with the name you gave your SharePoint iApp, followed by **_apm_access**.
3. On the Menu bar, click **SSO/Auth Domains**.
4. From the **SSO Configuration** list, select the NTLMv2 SSO Configuration you created.
5. Click **Update**.
6. You can optionally re-enable Strict Updates. Keep in mind, if you re-enter the iApp template and make changes to the configuration, you must perform this procedure again.

Next steps

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

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 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 configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, 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 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 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.

Troubleshooting

Q: Why do the SharePoint 2010 Document Library ribbon or Calendar options fail to load or get stuck on a status of **Loading...**?

A: Note: This issue has been fixed in version 1.1.0 of the iApp template. If you are using a previous version of the template, we strongly recommend upgrading to version 1.1 (see *Upgrading an Application Service from previous version of the iApp template on page 10)*. If you cannot upgrade, use the following guidance.

Deploying the HTTP Compression, OneConnect *and* NTLM profiles at the same time may prevent the SharePoint Document Library ribbon and calendar objects from loading. Additionally, **401 Unauthorized** responses may be seen for the ribbon object or calendar objects when analyzing HTTP traffic.

If you are using all three of these profiles on the same virtual server and are experiencing this issue, create the following iRule and attach to the SharePoint virtual server.

From the Main tab, expand **Local Traffic** and then click **iRules**. Click the **Create** button. Use the following code in the Definition section, omitting the line numbers:

```
when HTTP_RESPONSE {
    if {[HTTP::header exists "Transfer-Encoding"]} {
        HTTP::payload rechunk
    }
}
```

You may need to clear the browser's cache after attaching the iRule.

Adding the iRule to the virtual server

The final task is to add the iRule to the iApp configuration. If you manually configured the system, simply attach the iRule to the virtual server. If you used the iApp, use the following procedure.

To add the iRule to the SharePoint virtual server

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. In the iRules section, from the **Do you want to add any custom iRules to this configuration?** question, select the iRule you just created and then click the Add (**<<**) button to move it to the selected list.
5. Click the **Finished** button.

Q: Why am I unable to sync local files to SharePoint 2013 using the SkyDrive client and Office 2013 Upload Center?

A: If you have secured SharePoint 2013 with F5 Access Policy Manager, you must apply the following iRule to the SharePoint 2013 BIG-IP virtual server to allow file synchronization between the SharePoint site and SkyDrive/Office 2013 Upload Center clients.

From the Main tab, expand **Local Traffic** and then click **iRules**. Click the **Create** button. Use the following code in the Definition section, omitting the line numbers:

```
when HTTP_REQUEST {
    if { [string tolower [HTTP::header "User-Agent"]] contains "skydrive" || [string tolower [HTTP::header "User-Agent"]] contains "upload center" }  {
        ACCESS::disable
    }
}
```

Use the procedure *Adding the iRule to the virtual server* above to add the iRule to the virtual server.

Q: Why am I getting an error about an NTLM profile not being found when I try to submit the iApp template using RC 1 and RC 2?

A: If you are attempting to deploy the template using the F5 recommended NTLM profile (a default setting for 2010, the default is none if you are using 2013) and are deploying the template in an administrative partition, you will receive an error about the NTLM profile not being found. This is no longer an issue using RC 3 or v1.0.0 and v1.1.0. We recommend using the latest version of the iApp template.

If you cannot use RC 3 or the supported v1.0.0 or 1.1.0 release, and are deploying in a partition other than the default /Common partition, before you configure the iApp template, you need to create an NTLM profile, then run the template and for the question *Which NTLM profile do you want to use?* select the profile you created.

To create a new NTLM profile, go to **Local Traffic > Profiles > Other > NTLM** and then click **Create**. Leave all settings at the default, and then click **Finished**.

After creating the profile, start the SharePoint iApp template. Configure the settings as applicable for your configuration, making sure to select the NTLM profile you created for the answer to the *Which NTLM profile do you want to use?* question.

Q: Why are users experiencing authentication issues after deploying the SharePoint iApp template?

A: If the OneConnect feature is used with a SharePoint web application that is configured for Kerberos authentication, AND the SharePoint servers are using Windows 2012 or 2012 R2 (or if using Windows 2008 R2, the *AuthPersistNonNTLM* value is set to true), clients may experience issues with authentication after deploying the iApp template for either SharePoint 2010 or 2013.

To solve this issue, we recommend creating the following iRule that selectively disables the OneConnect profile, and then reconfiguring the iApp to attach the iRule to the virtual server.

From the Main tab, expand **Local Traffic** and then click **iRules**. Click the **Create** button. Use the following code in the Definition section, omitting the line numbers:

```
when HTTP_REQUEST {
    set iskrb 0
    if { [HTTP::header exists "Authorization"] } {
        if { [string tolower [HTTP::header "Authorization"]] starts_with "negotiate y" }  {
            set iskrb 1
        }
    }
}

when HTTP_RESPONSE {
    if { [HTTP::header exists "Persistent-Auth"] } {
        if { $iskrb == 1 && [string tolower [HTTP::header "Persistent-Auth"]] contains "true" }  {
            ONECONNECT::reuse disable
            ONECONNECT::detach disable
            log local0.  "OneConnect disabled"
        }
    }
    unset iskrb
}
```

After creating the iRule, attach the iRule to the SharePoint virtual server. If you created the configuration manually, simply add the iRule to the virtual server in the Configuration utility. If you used the iApp template, use the following procedure.

Adding the iRule to the virtual server

The final task is to add the iRule to the iApp configuration.

To add the iRule to the SharePoint virtual server

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. In the iRules section, from the *Do you want to add any custom iRules to this configuration?* question, select the iRule you just created and then click the Add (**<<**) button to move it to the selected list.
5. Click the **Finished** button.

Q: After deploying the iApp, why are users receiving an error when trying to modify the view of a SharePoint list, or the **Connect to Outlook** button is greyed out?

A: This is typically a result of using SharePoint's *Minimal Download Strategy* feature with the default BIG-IP configuration. SharePoint 2013 sites configured with the Minimal Download Strategy feature return incorrect HTTP responses when the BIG-IP HTTP compression profile removes the Accept-Encoding header from the request.

To solve this issue, we recommend deactivating Minimal Download Strategy from the SharePoint **Site Settings > Manage Site Features** page. See the Microsoft documentation for specific instructions.

Alternatively, you can create a custom compression profile on the BIG-IP system with **Keep Accept-Encoding** enabled, and then select it within the iApp template.

To create a new HTTP Compression profile, go to **Local Traffic > Profiles > Services > HTTP Compression** and then click **Create**. In the **Keep Accept Encoding** row, click the Custom box, and then click the **Keep Accept Encoding** box to ensure the system does not remove this header. Click **Finished**.

To add the profile to the SharePoint virtual server

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. If necessary, from the *Which configuration mode do you want to use?* question, select **Advanced - Configure advanced options**.
5. In the Delivery Optimization section, from the *Which compression profile do you want to use?* question, select the profile you created.
6. Click the **Finished** button.

Q: Why are users unable to open SharePoint document libraries in Windows Explorer or edit SharePoint documents in Microsoft Office applications after deploying the BIG-IP APM?

A: When accessing SharePoint Server 2010 or 2013 through BIG-IP APM, you may encounter errors when attempting to open document libraries with Windows Explorer. Additionally, you may be unable to open or save Microsoft Office documents located in a SharePoint document library. This behavior can occur when the Microsoft WebDAV client fails to send the persistent APM session cookie with every request.

To correct this behavior, download and install the following hotfix from Microsoft on client computers exhibiting the issue: *http://support.microsoft.com/kb/2936341*. A system restart may be necessary after installation.

Q: Why are client connections unresponsive or seem to hang when using the OneConnect feature?

A: If you have configured your deployment to use OneConnect (part of F5's recommended configuration), and users are experiencing slow performance or the need to refresh pages, Microsoft IIS may be failing to reset the TCP connection after the default timeout period of 120 seconds.

To work around this issue, create a custom server-side TCP profile with an **Idle Timeout** value of less that 120 seconds, and then apply the profile to the virtual server. If you used the iApp template to configure the BIG-IP system, you can attach the new profile using the template. If you manually configured the BIG-IP system, you manually add the profile.

To create the new TCP profile, click **Local Traffic > Profiles > Protocol > TCP** and then click **Create**. From the Parent Profile list, select **tcp-lan-optimized**. Check the Custom box for **Idle Timeout**, and then in the **Seconds** box, type a number less than 120, such as **110.** Click **Finished** to create the profile.

To add the profile to the SharePoint virtual server

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. If necessary, from the *Which configuration mode do you want to use?* question, select **Advanced - Configure advanced options**.
5. In the Server Offload section, from the *Which OneConnect profile do you want to use?* question, select the profile you just created.
6. Click the **Finished** button.

If you configured the BIG-IP system manually, simply replace the existing **Protocol Profile (Server)** profile with the profile you just created.

Q: I entered multiple FQDNs in the Virtual Server and Pools section of the iApp, so why does APM Single Sign-On only work for the first FQDN?

A: If you are running BIG-IP version 11.5.x, deployed BIG-IP APM, and entered more than one application FQDN, the BIG-IP APM sends a TCP reset in response to requests for the additional authentication domains.

This is a known issue in BIG-IP version 11.5 and 11.5.1, and has been fixed in BIG-IP v11.5.0 HF 5 and BIG-IP 11.5.1 HF 5. You must upgrade the BIG-IP system to one of these hotfixes (or later version).

See *https://support.f5.com/kb/en-us/solutions/public/13000/100/sol13123* for instructions on downloading and installing BIG-IP system hotfixes.

Q: I configured the iApp template to use AFM to Reject or Log access connections from sources with low reputation scores, why isn't the system rejecting or logging those connections?

A: This is a known issue with the iApp template. If you are using BIG-IP AFM and IP Intelligence, and configured the iApp template to log or reject connection attempts from sources with a low reputation scores, you must configure the Blacklist categories manually before connections are logged or rejected. Use the following guidance.

1. Disable Strict Updates if you have not already. See *To disable Strict Updates on page 32.*
2. Click **Security > Network Firewall > IP Intelligence > Policies >** *(name-you-gave-the-iApp)***_ip_intelligence**.
3. In the Blacklist Matching Policy area, from the **Blacklist Category** list, select a category that you want to log or reject, and then click **Add**.
4. Repeat step 3 to add all applicable blacklist categories.
5. Click Update.
6. You can optionally re-enable Strict Updates. Keep in mind, if you re-enter the iApp template and make changes to the configuration, you must perform this procedure again.

Appendix A: Configuring SharePoint Alternate Access Mappings to support SSL offload

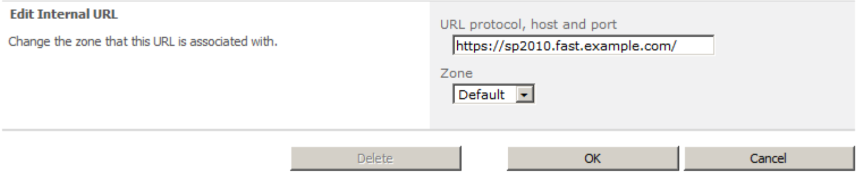
When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the BIG-IP LTM SSL virtual server and ensure correct rewriting of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



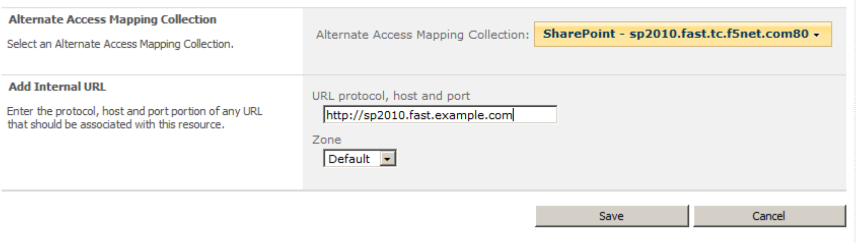
Edit Internal URL

Change the zone that this URL is associated with.

URL protocol, host and port: https://sp2010.fast.example.com/

Zone: Default

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.



Alternate Access Mapping Collection

Select an Alternate Access Mapping Collection.

Alternate Access Mapping Collection: SharePoint - sp2010.fast.tc.f5net.com80

Add Internal URL

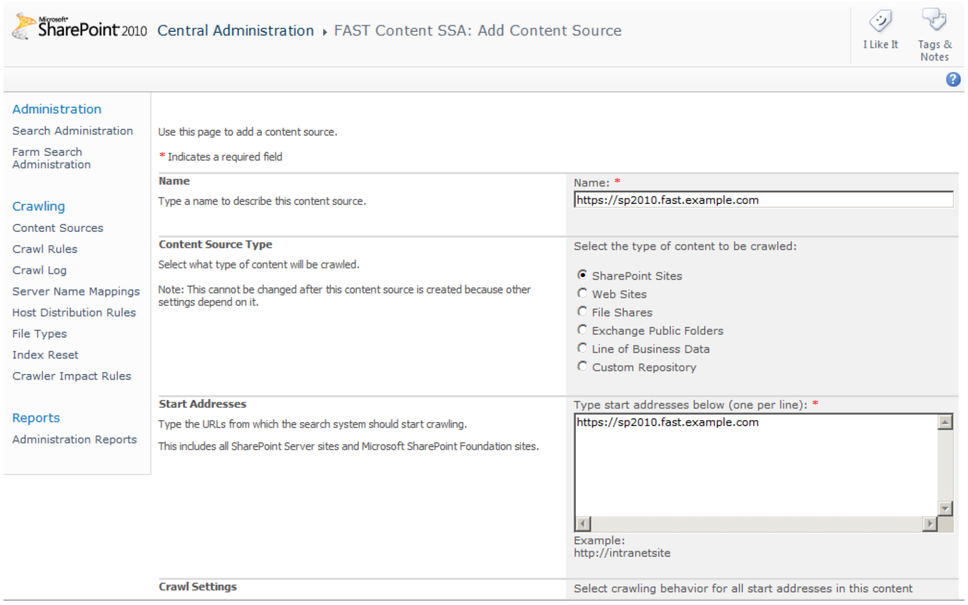
Enter the protocol, host and port portion of any URL that should be associated with this resource.

URL protocol, host and port: http://sp2010.fast.example.com

Zone: Default

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://sp2010.fast.example.com**.
14. 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.
15. Click the **OK** button.
16. Repeat this entire procedure for each public URL to be deployed behind LTM.



Use this page to add a content source.

* Indicates a required field

Name
Type a name to describe this content source.

Name: *
https://sp2010.fast.example.com

Content Source Type
Select what type of content will be crawled.

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

Select the type of content to be crawled:
● SharePoint Sites
○ Web Sites
○ File Shares
○ Exchange Public Folders
○ Line of Business Data
○ Custom Repository

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

This includes all SharePoint Server sites and Microsoft SharePoint Foundation sites.

Type start addresses below (one per line): *
https://sp2010.fast.example.com

Example:
http://intranetsite

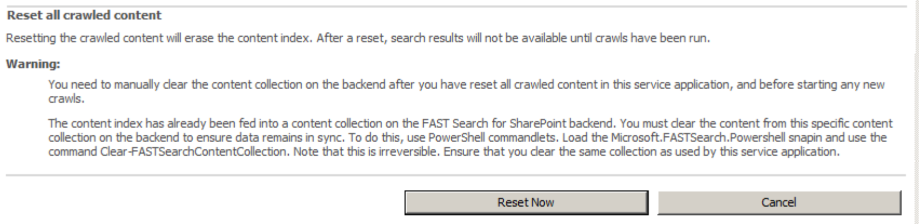
Crawl Settings
Select crawling behavior for all start addresses in this content

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

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.



Reset all crawled content

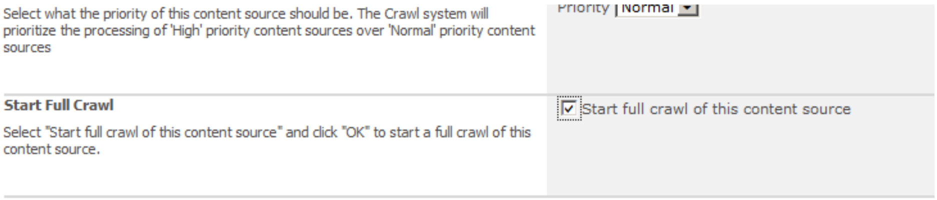
Resetting the crawled content will erase the content index. After a reset, search results will not be available until crawls have been run.

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.

Appendix B: Manual configuration tables

We strongly recommend using the iApp template to configure the BIG-IP system for Microsoft SharePoint. Users familiar with the BIG-IP system can use the following table to manually configure the BIG-IP system. The table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. Settings not mentioned 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 *(Local Traffic > Monitors)*	***Name***	Type a unique name	
	Type	**HTTP** (**HTTPS** if you are deploying SSL Bridging)	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Send String	Optional. We use **GET / HTTP/1.1\r\nHost:** *<FQDN clients use for access>***\r\nConnection: Close\r\n\r\n**	
	Receive String	**200 OK** If you configured your SharePoint web application to use AD FS as a Trusted Identity authentication provider, see *Optional: Monitoring SharePoint Web Applications Configured for AD FS as a Trusted Identity Provider on page 30*	
Pool *(Local Traffic > Pools)*	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300** (recommended)	
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)	
	Address	Type the IP Address of the nodes	
	Service Port	**80** (**443** if configuring SSL Bridging). Click **Add** to repeat Address and Service Port for all nodes)	
***Optional*: AAM Application**[2] *(Acceleration > Web Application)*	***Application Name***	Type a unique name	
	Policy	**Microsoft SharePoint 2010**	
	Requested Host	Type the FQDN of your application. Click **Add Host** to include more hosts. If you are also deploying the system for SharePoint Apps, or have Office Web Apps accessed through the virtual server you must add those FQDNs.	
***Optional*: APM**[2]	See *Manually configuring the BIG-IP APM for SharePoint on page 47* for the BIG-IP APM configuration objects		
Profiles *(Local Traffic > Profiles)*	***HTTP*** *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**http**
		Rewrite Redirect[2]	**Matching**
	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** **Do not create this profile if using SharePoint 2013**
	OneConnect *(Profiles > Other)*	Name	Type a unique name
		Parent Profile	**oneconnect**
		Source Mask	**SharePoint 2013 only: 0.0.0.0**
	Client SSL[3] *(Profiles > SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Server SSL[4] *(Profiles > Other)*	Name	Type a unique name
		Parent Profile	**serverssl**
	Web Acceleration *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**optimized-caching**
		WA Applications[2]	Enable the AAM Application you created
	iSession[5] *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**isession**

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

[2] *Optional. The BIG-IP AAM configuration is recommended, but optional. BIG-IP APM is optional.*

[3] *Only required if using the BIG-IP system for SSL Offload or SSL Bridging*

[4] *Only necessary if using the BIG-IP system for SSL Bridging or server-side encryption*

[5] *Only necessary if using the BIG-IP AAM to provide symmetric optimization*

<table>
<tr><th>BIG-IP LTM Object</th><th colspan="3">Non-default settings/Notes</th></tr>
<tr><td rowspan="5">**Profiles**
(Local Traffic > Profiles)</td><td rowspan="5">***HTTP Compression***
(Profiles > Services)</td><td>Name</td><td>Type a unique name</td></tr>
<tr><td>Parent Profile</td><td>**wan-optimized-compression**</td></tr>
<tr><td rowspan="3">Content List--> Include List
(Copy and paste each entry to the ***Content Type*** *box and click* ***Include****.)*</td><td>text/(css|html|javascript|json|plain|postscript|richtext|rtf|vnd\.wap\.wml|vnd\.wap\.wmlscript|wap|wml|x-component|x-vcalendar|x-vcard|xml)</td></tr>
<tr><td>application/(css|css-stylesheet|doc|excel|javascript|json|lotus123|mdb|mpp|ms-excel|ms-powerpoint|ms-word|msaccess|msexcel|mspowerpoint|msproject|msword|photoshop|postscript|powerpoint|ps|psd|quarkexpress|rtf|txt|visio|vnd\.excel|vnd.\ms-access|vnd\.ms-excel|vnd\.ms-powerpoint|vnd\.ms-pps|vnd\.ms-project|vnd\.ms-word|vnd\.ms-works|vnd\.ms-works-db|vnd\.msaccess|vnd\.msexcel|vnd\.mspowerpoint|vnd\.msword|vnd\.powerpoint|vnd\.visio|vnd\.wap\.cmlscriptc|vnd\.wap\.wmlc|vnd\.wap\.xhtml\+xml|vnd\.word|vsd|winword|wks|word|x-excel|x-java-jnlp-file|x-javascript|x-json|x-lotus123|x-mdb|x-ms-excel|x-ms-project|x-mscardfile|x-msclip|x-msexcel|x-mspowerpoint|x-msproject|x-msword|x-msworks-db|x-msworks-wps|x-photoshop|x-postscript|x-powerpoint|x-ps|x-quark-express|x-rtf|x-vermeer-rpc|x-visio|x--vsd|x-wks|x-word|x-xls|x-xml|xhtml+xml|xls|xml)</td></tr>
<tr><td>image/(photoshop|psd|x-photoshop|x-vsd)</td></tr>
<tr><td rowspan="16">**Virtual Servers**
(*Local Traffic > Virtual Servers*)</td><td colspan="3">**HTTP**</td></tr>
<tr><td>***Name***</td><td colspan="2">Type a unique name.</td></tr>
<tr><td>***Address***</td><td colspan="2">Type the IP Address for the virtual server</td></tr>
<tr><td>***Service Port***</td><td colspan="2">**80**</td></tr>
<tr><td>***Protocol Profile (client)***[1,2]</td><td colspan="2">Select the WAN optimized TCP profile you created above</td></tr>
<tr><td>***Protocol Profile (server)***[1,2]</td><td colspan="2">Select the LAN optimized TCP profile you created above</td></tr>
<tr><td>***HTTP Profile***[2]</td><td colspan="2">Select the HTTP profile you created above</td></tr>
<tr><td>***Web Acceleration profile***[2]</td><td colspan="2">Select the Web Acceleration profile you created above</td></tr>
<tr><td>***HTTP Compression profile***[2]</td><td colspan="2">Select the HTTP Compression profile you created above</td></tr>
<tr><td>***OneConnect***[2]</td><td colspan="2">Select the OneConnect profile you created above</td></tr>
<tr><td>***Source Address Translation*** [3]</td><td colspan="2">**Auto Map** (optional; see footnote [3])</td></tr>
<tr><td>***Access Policy***[2]</td><td colspan="2">If you deployed BIG-IP APM only: Select the Access Policy you created. See the next page for details.</td></tr>
<tr><td>**iSession profile**[5]</td><td colspan="2">If using BIG-IP AAM for symmetric optimization between systems, select the iSession profile you created.</td></tr>
<tr><td>***Default Pool***[2]</td><td colspan="2">Select the pool you created above</td></tr>
<tr><td>***Persistence Profile***[2]</td><td colspan="2">Select the Persistence profile you created</td></tr>
<tr><td>***iRule***</td><td colspan="2">If offloading SSL only: Enable the built-in **_sys_https_redirect irule**</td></tr>
<tr><td rowspan="17">**Virtual Servers**
(*Local Traffic > Virtual Servers*)</td><td colspan="3">**HTTPS**[4]</td></tr>
<tr><td>***Name***</td><td colspan="2">Type a unique name.</td></tr>
<tr><td>***Address***</td><td colspan="2">Type the IP Address for the virtual server</td></tr>
<tr><td>***Service Port***</td><td colspan="2">**443**</td></tr>
<tr><td>***Protocol Profile (client)***[1]</td><td colspan="2">Select the WAN optimized TCP profile you created above</td></tr>
<tr><td>***Protocol Profile (server)***[1]</td><td colspan="2">Select the LAN optimized TCP profile you created above</td></tr>
<tr><td>***HTTP Profile***</td><td colspan="2">Select the HTTP profile you created above</td></tr>
<tr><td>***Web Acceleration profile***</td><td colspan="2">Select the Web Acceleration profile you created above</td></tr>
<tr><td>***HTTP Compression profile***</td><td colspan="2">Select the HTTP Compression profile you created above</td></tr>
<tr><td>***OneConnect***</td><td colspan="2">Select the OneConnect profile you created above</td></tr>
<tr><td>***SSL Profile (Client)***</td><td colspan="2">Select the Client SSL profile you created above</td></tr>
<tr><td>***SSL Profile (Server)***[6]</td><td colspan="2">If you created a Server SSL profile, select it from the list</td></tr>
<tr><td>***Source Address Translation*** [3]</td><td colspan="2">**Auto Map** (optional; see footnote [3])</td></tr>
<tr><td>***Access Policy***</td><td colspan="2">If you deployed BIG-IP APM only: Select the Access Policy you created. See the next page for details.</td></tr>
<tr><td>**iSession profile**[5]</td><td colspan="2">If using BIG-IP AAM for symmetric optimization between systems, select the iSession profile you created.</td></tr>
<tr><td>***Default Pool***</td><td colspan="2">Select the pool you created above</td></tr>
<tr><td>***Persistence Profile***</td><td colspan="2">Select the Persistence profile you created</td></tr>
</table>

[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.*

[3] *If expecting more than 64,000 simultaneous connections per server, you must configure a SNAT Pool. See the BIG-IP documentation on configuring SNAT Pools.*

[4] *This virtual server is only necessary if offloading SSL or SSL Bridging*

[5] *Only necessary if using the BIG-IP AAM to provide symmetric optimization. Do not create/use this profile if you are deploying the BIG-IP system on the server side of the WAN*

[6] *Only necessary if using the BIG-IP system for SSL Bridging or server-side encryption*

Manually configuring the BIG-IP APM for SharePoint

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.

If you have already configured the BIG-IP LTM virtual server, after configuring APM, you must modify the virtual server and add the Access profile you create in this section.

BIG-IP Object	Non-default settings/Notes	
DNS and NTP	See *Appendix C: Configuring additional BIG-IP settings on page 56 for instructions on configuring DNS and NTP on the BIG-IP system.*	
Health Monitor[1] (*Local Traffic--> Monitors*) **Note:** Only necessary if creating a pool of Active Directory servers	***Configuration***	Select **Advanced** from the Configuration list (if necessary).
	Name	Type a unique name, such as AD_LDAP_monitor.
	Type	**LDAP**
	Interval	**10** (recommended)
	Timeout	**31** (recommended)
	User Name	Type a user name with administrative permissions
	Password	Type the associated password
	Base	Specify your LDAP base tree. For example, CN=SharePoint Users,DC=example,DC=com
	Filter	Specify the filter. We type **cn=user1**, using the example above: user1 in OU group "SharePoint Users" and domain "example.com"
	Security	Select a Security option (either None, SSL, or TLS)
	Chase Referrals	**Yes**
	Alias Address	***All Addresses**
	Alias Address Port	**389** (for None or TLS) or **686** (for SSL)
AAA Server (*Access Policy-->AAA Servers*)	***If you are using a single Active Directory Server***	
	Name	Type a unique name. We use **sharepoint-aaa-server**.
	Type	**Active Directory**
	Domain Controller	Type the IP address or FQDN name of an Active Directory Domain Controller
	Domain Name	Type the Active Directory domain name
	Admin Name[1]	Type the AD user name with administrative permissions (optional)
	Admin Password[1]	Type the associated password (optional). Type it again in the Verify Password box
	If you are using a pool of Active Directory Servers	
	Name	Type a unique name. We use **sharepoint-aaa-server**.
	Type	**Active Directory**
	Domain Name	Type the FQDN of the Windows Domain name
	Server Connection	Click **Use Pool** if necessary.
	Domain Controller Pool Name	Type a unique name
	Domain Controllers	**IP Address**: Type the IP address of the first domain controller **Hostname**: Type the FQDN of the domain controller Click **Add**. Repeat for each domain controller in this configuration.
	Server Pool Monitor	Select the monitor you created above.
	Admin Name[2]	Type the Administrator name
	Admin Password[2]	Type the associated password
SSO Configurations *(Access Policy-->SSO Configurations)*	***NTLM SSO Configuration*** *(use this if you are deploying BIG-IP APM for NTLM authentication)*	
	Name	Type a unique name. We use **sharepoint-ntlm-sso**.
	SSO Method	**NTLMv1**
	NTLM Domain	The NTLM domain name where the user accounts are located

[1] Only necessary if using a pool of Active Directory servers

[2] Optional; Admin Name and Password are only required if anonymous binding to Active Directory is not allowed in your environment

BIG-IP Object	Non-default settings/Notes	
SSO Configurations *(Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar))*	***Smart Card SSO Configuration*** *(use this if you are deploying BIG-IP APM for Smart Card authentication)*	
	Name	Type a unique name. We use **smart-card-SSO**.
	SSO Method	**Kerberos**
	Username Source	**session.logon.last.username**
	User Realm Source	**session.logon.last.domain**
	Kerberos Realm	Type your SharePoint Kerberos Realm in all caps
	KDC	Type the IP address or FQDN of Active Directory domain controller
	Account Name	Type the Active Directory account user name for APM delegation in SPN format
	Account Password	Type the associated password
	Confirm Account Password	Confirm the password
	Send Authorization	**Always**
Access Profile *(Main tab-->Access Policy-->Access Profiles)*	***Name***	Type a unique name.
	Restrict to Single Client IP[1]	Enable this feature for additional security when using the Persistent cookie setting.
	Logout URI Include	SharePoint 2010: **/_layouts/SignOut.aspx** SharePoint 2013: **/_layouts/15/SignOut.aspx**
	Cookie Options	Click a check in the **Persistent Cookie** box
	SSO Configuration	Select the appropriate SSO Configuration you created.
	Languages	Move the appropriate language(s) to the **Accepted** box.
Access Policy *(See procedure below)*	*Edit*	Edit the Access Profile you just created using the Visual Policy Editor Continue now with configuring the Access policy below.

[1] 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

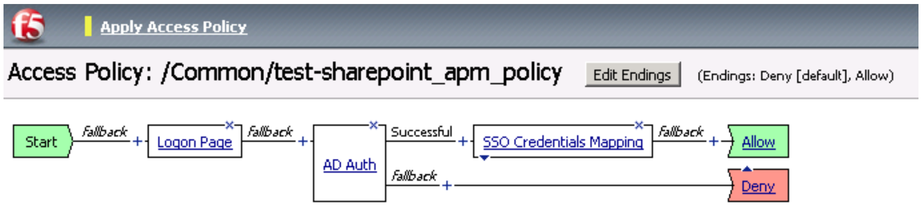
The next step is to edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. This policy is just an example, you can use it or create one of your own.

The Access Policy is different depending on which SSO Configuration (NTLM or Smart Card) you configured.

Editing the Access Policy for NTLM authentication

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 **Save**.
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.
14. Click the **Close** button on the upper right to close the VPE.



Apply Access Policy

Access Policy: /Common/test-sharepoint_apm_policy Edit Endings (Endings: Deny [default], Allow)

This completes the configuration for NTLM authentication.

Editing the Access Policy for smart card authentication

1. On the Main tab, expand **Access Policy**, and 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 **Client Cert Inspection** option button, and then click **Add Item**.
   a. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
   b. Click the **Save** button.
5. On the *Successful* path between **Client Cert Inspection** and **Deny**, click the **+** symbol The options box opens
6. Click the **Variable Assign** option button, and then click **Add Item**. It is important you add the variables in the following order.
   a. Click **Add new entry**.
   b. Click the **Change** link on the new entry.
   c. In the **Custom Variable** box, type **: session.logon.last.domain**.
   d. In the **Custom Expression** box, type

   ```
   session.logon.last.domain = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn [expr { [string first "@" $upn] + 1 } ] end ]; } else { return ""; }
   ```

   e. Click **Finished**.
   a. Click **Add new entry**.
   b. Click the **Change** link on the new entry.
   c. In the **Custom Variable** box, type **session.logon.last.username**.
   d. In the **Custom Expression** box, type

   ```
   session.logon.last.username = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn 0 [expr { [string first "@" $upn] - 1 } ] ]; } else { return $upn; }
   ```

   e. Click **Finished**.
   a. Click **Add new entry**.
   b. Click the **Change** link on the new entry.

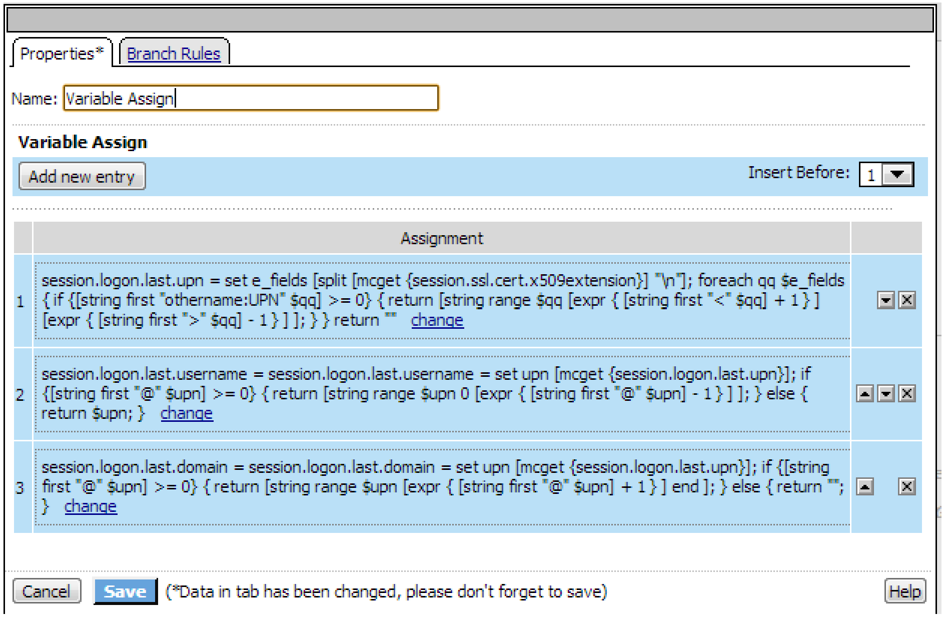
c. In the **Custom Variable** box, type **session.logon.last.upn**.

d. In the **Custom Expression** box, type

```
set e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"]; foreach qq $e_fields { if
{[string first "othername:UPN" $qq] >= 0} { return [string range $qq [expr { [string first "<" $qq]
+ 1 } ] [expr { [string first ">" $qq] - 1 } ] ]; } } return ""
```

e. Click **Finished**.

f. Click **Save**.
When you are finished, your Variable Assign item must look like the following example. Use the arrows on the right to move the variables if necessary.



Name: Variable Assign

Variable Assign

Insert Before: 1

	Assignment
1	session.logon.last.upn = set e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"]; foreach qq $e_fields { if {[string first "othername:UPN" $qq] >= 0} { return [string range $qq [expr { [string first "<" $qq] + 1 }] [expr { [string first ">" $qq] - 1 }]]; } } return "" change
2	session.logon.last.username = session.logon.last.username = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn 0 [expr { [string first "@" $upn] - 1 }]]; } else { return $upn; } change
3	session.logon.last.domain = session.logon.last.domain = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn [expr { [string first "@" $upn] + 1 }] end]; } else { return ""; } change

(*Data in tab has been changed, please don't forget to save)

7. Click the **+** symbol between **Variable Assign** and **Deny**. The options box opens.

8. Click the **SSO Credential Mapping** option button, and then click **Add Item**.

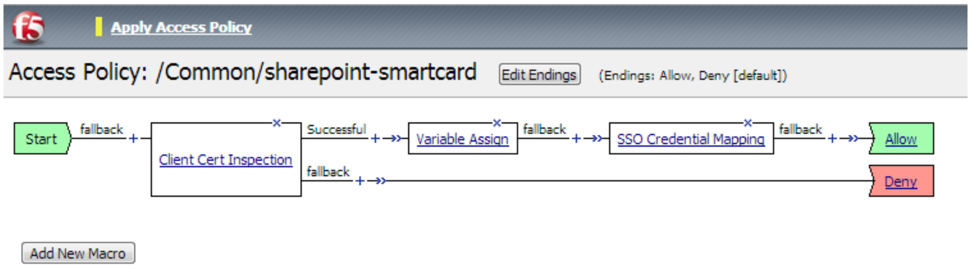
9. Click the **Save** button.

10. On the fallback path between **SSO Credential Mapping** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.

11. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.

12. Click the **Close** button on the upper right to close the VPE.

When you are finished, the Access Policy should look like the following example.



Access Policy: /Common/sharepoint-smartcard

(Endings: Allow, Deny [default])

Manually configuring the BIG-IP Advanced Firewall Module to secure your SharePoint deployment

This section describes how to manually configure BIG-IP AFM, F5's Network Firewall module, to secure your SharePoint deployment. BIG-IP AFM is particularly useful if you want to only allow access from specific clients or networks. Because this configuration can be complex, we recommend using the iApp template in version 11.6 and later to configure BIG-IP AFM.

Network Firewall settings

When configuring the BIG-IP Advanced Firewall Manager, you may want to configure your BIG-IP system to drop all traffic that you have not specifically allowed with firewall rules. This in known as ***firewall mode***. By default, your BIG-IP system is set to default-accept, or ***ADC mode***. Instructions for configuring your BIG-IP system, and the implications to consider, can be found on AskF5. For example, for BIG-IP v11.5: *http://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/1.html*

If you have licensed IP Intelligence on the BIG-IP system, you can prohibit connections from sources with low reputation scores.

The following instructions cover a basic firewall configuration that is effective for the most common scenario of wanting to allow connections from a single trusted network. If you have complex requirements, such as the need to schedule different policies for different times of the day, or you want to create complicated rule or address lists, consult the BIG-IP AFM documentation. The basic steps for Policy and Rule creation apply to all scenarios.

To configure the BIG-IP AFM to allow connections from a single trusted network

1. Create a Network Firewall Policy:
   a. From the Configuration utility, click **Security > Network Firewall > Policies**, and then click **Create**.
   b. In the **Name** field, type a unique name for the policy, such as **SharePoint-Policy**.
   c. Click **Finished**.

2. Create a rule to allow authorized hosts or networks to connect:
   a. Click **Security > Network Firewall > Policies**.
   b. Click the name of the policy you just created.
   c. In the Rule section (below the General Properties section), click the **Add** button.
   d. Leave the **Type** list set to Rule.
   e. From the **Order** list, select **First**. The Order list only appears in version 11.5 and later. In 11.4.x, you must reorder the rules from the Policy General Properties page.
   f. In the **Name** field, type a unique name, for instance **SharePoint-traffic-Allowed**.
   g. Ensure the **State** list is set to **Enabled**.
   h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.
   i. In the **Source** section, from the **Address/Region** list, select **Specify**.
   You are now able to list the trusted source addresses for your connection.
   In the following example, we will configure a single subnet as trusted.
      - Select **Address**.
      - In the box, type the network address you want to allow, including netmask if more than a single host. Specify a network using CIDR notation, such as **10.0.0.0/24**.
      - Do not configure a source port.
      - Optional: If you want to limit inbound connections to a specific VLAN or Tunnel, from the **VLAN / Tunnel** list, select **Specify**, and then move the VLANs or tunnels that are allowed access to the Selected box.
      - Click **Add**.
      - Repeat these steps for additional hosts or networks. Use **Address List** or **Address Range** when appropriate.

   j. In the **Destination** section, leave the **Address/Region** and **Port** set to **Any**. Because you will be applying your policy to a virtual server that listens only on a single desired address and port, do not specify that information here.
   k. If necessary, from the **Action** list, select **Accept**.

l. *Optional:* If you have configured a logging profile and want to log connections, from the **Logging** list, select **Enabled**. Typically, allowed connections do not need to be logged.

m. Click **Finished**.

3. Creating a firewall rule to block all other traffic
The next task is to create a firewall rule to block all other traffic that you have not allowed. Although this is not a required step if your BIG-IP system is set to default deny (**Firewall mode**), it is required in default-accept (**ADC mode**), and is a good practice to always configure such a rule.

a. Click **Security > Network Firewall > Policies**.

b. Click the name of the policy you created in step 1.

c. In the Rule section (below the General Properties section), click the **Add** button.

d. Leave the **Type** list set to **Rule**.

e. Leave the **Order** list, select **Last**.

f. In the **Name** field, type a unique name, for example **SharePoint-traffic-Prohibited**.

g. Ensure the **State** list is set to **Enabled**.

h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.

i. In the **Source** section, leave all the lists set to **Any**

j. From the **Action** list, select either **Drop** (to silently discard incoming connections) or **Reject** (to send a Destination Unreachable message to the sender).

k. If you configured a logging profile as described in *Optional: Configuring the BIG-IP system to log network firewall events on page 53*, from the **Logging** list, select **Enabled**.

l. Click **Finished**. You return to the Policy Properties page.

m. On the Policy Properties page, in the Rules section, ensure the rule with the Action of Accept comes before the Drop or Reject rule you just created. If it does not, use the **Reorder** button and drag the rules into the correct order.

4. Apply Your Firewall Policy to your Virtual Server

a. Click **Security > Network Firewall > Active Rules**.

b. In the Rule section (below the General Properties section), click the **Add** button.

c. From the **Context** list, select **Virtual Server**, and then select the virtual server you created for your SharePoint traffic.

d. From the **Type** list, select **Policy**, and then select the firewall policy you created.

e. From the **Policy Type** list, select **Enforced**.

f. Click **Finished**.

Optional: Assigning an IP Intelligence Policy to your SharePoint virtual server

If you want to restrict access to your SharePoint virtual server based on the reputation of the remote sender, you can enable and assign an IP Intelligence policy. This requires an IP intelligence license; contact your F5 Sales representative for more information.

It is outside the scope of this document to provide instructions on configuring an IP Intelligence Policy. Full documentation on enabling and configuring the IP Intelligence feature can be found on AskF5. For example, the manual for BIG-IP AFM v11.5 is:
https://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/5.html

After you have enabled and configured an IP Intelligence policy, use the following steps to assign the policy to your SharePoint virtual server:

To assign the IP intelligence policy to the SharePoint virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your SharePoint virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **IP Intelligence**, select **Enabled**, then select the IP intelligence policy to apply to traffic on the virtual server.
5. Click **Update**. The list screen and the updated item are displayed. The IP Intelligence policy is applied to traffic on the virtual server.

Optional: Configuring the BIG-IP system to log network firewall events

If you are using BIG-IP AFM, you have the option of logging network firewall events to one or more remote syslog servers (recommended) or to log events locally. You can either use an iApp template to create the logging profile, or create the logging profile manually.

For specific information on logging on the BIG-IP system, see the appropriate guide for your version. For example, for 11.5.0:

- Remote High-Speed Logging:
  https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-5-0/22.html
- Local logging:
  https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-concepts-11-5-0/11.html

Creating the logging profile using the iApp template

Use this section to create the logging profile using the logging profile iApp template. If you have not already downloaded the iApp template, see *https://devcentral.f5.com/wiki/iApp.F5-Remote-Logging-iApp.ashx*.

To configure the logging profile iApp

1. Log on to the BIG-IP system.
2. On the Main tab, click **iApp > Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **logging-iapp_.**
5. From the **Template** list, select **f5.remote_logging.v<*latest-version*>**. The template opens
6. Use the following table for guidance on configuring the iApp template. Questions not mentioned in the table can be configured as applicable for your implementation.

Question	Your selection
Do you want to create a new pool of remote logging servers, or use an existing one?	Unless you have already created a pool on the BIG-IP system for your remote logging servers, select **Create a new pool**.
Which servers should be included in this pool?	Specify the IP addresses of your logging servers. Click **Add** to include more servers.
What port do the pool members use?	Specify the port used by your logging servers, typically **514**.
Do the pool members expect UDP or TCP connections?	**TCP**
Do you want to create a new monitor for this pool, or use an existing one?	Unless you have already created a health monitor for your pool of logging servers, select **Use a simple ICMP (ping) monitor**.
Do your log pool members require a specific log format?	If your logging servers require a specific format, select the appropriate format from the list.

7. Click **Finished**.
8. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
9. Click the name of your SharePoint virtual server.
10. From the **Security** menu, choose **Policies**.
11. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.

12. Click **Update**. The list screen and the updated item are displayed.

> ***Note***
>
> *The iApp template creates a log publisher and attaches it to the logging profile. If the publisher does not appear in the BIG-IP Configuration utility (GUI), you can verify the configuration by running the following command from the Traffic Management shell (tmsh):* **`list security log profile <your profile name>`**.

Creating logging profile manually

If you do not want to use the iApp template to create a logging profile, use this section for guidance on configuring the logging profile manually. You must have access to the tmsh command line to use this method.

To manually configure a logging profile

1. Use the following guidance for configuring a health monitor and load balancing pool for the logging servers.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the appropriate monitor you created
	Slow Ramp Time	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of a server.
	Service Port	Type the appropriate port, such as UDP port **514**, the port on which logging typically occurs. Click **Add**, and then repeat Address and Port for all nodes

2. Log into the BIG-IP system using the command line. Enter the tmsh shell, by typing **tmsh** from the prompt.

3. Create a Remote High Speed Log (HSL) destination:

```
(tmos)# create / sys log-config destination remote-high-speed-log [name] pool-name [specified pool] protocol [udp or tcp]
```

4. If you have a specific log format requirement, create a format-specific log destination, and forward that to the previously-created HSL destination:

```
(tmos)# create / sys log-config destination [splunk|arcsight|remote-high-speed-log] [name] forward-to [HSL name]
```

5. Create a log publisher:

```
(tmos)# create / sys log-config publisher [name] destinations add { [logdestination name] }
```

6. Create the logging profile to tie everything together.
If you chose to log allowed connections, include the green text (as in step 2 substep I in *To configure the BIG-IP AFM to allow connections from a single trusted network on page 51)*.
If you set the rule to drop incoming connections, include the text in blue.
If you chose to log IP intelligence events, include the text in red to add the parameter that sets the log publisher.

```
(tmos)# create / security log profile [name] network add { [name] { filter { log-acl-match-accept enabled log-acl-match-drop enabled log-acl-match-reject enabled } format { field-list { date_time action drop_reason protocol src_ip src_port dest_ip dest_port } type field-list } publisher [logpublisher name] } } ip-intelligence { log-publisher
[logpublisher_name] }
```

Assigning the logging profile to the virtual server

The final task is to assign the logging profile to the virtual server.

To assign the logging profile to the SharePoint virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your SharePoint virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
5. Click **Update**. The list screen and the updated item are displayed.

Appendix C: Configuring additional BIG-IP settings

This section contains information on configuring the BIG-IP system for objects or settings that are required, but not part of the template.

Configuring DNS and NTP settings

If you are configuring the iApp to use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the iApp.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

➡ ***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 self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. 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 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.

Appendix D: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional)

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 Auto Map), 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. The iApp produces an HTTP profile on the BIG-IP system which inserts an X-Forwarded-For header, so 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.

Modifying the iApp to insert the X-Forwarded-For header if necessary

First, you must make sure you have enabled the iApp to insert the X-Forwarded-For header. To change or verify the value of this setting, use the following procedure.

To insert the X-Forwarded-For header.

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the list, click the name of the SharePoint Application Service you created.
3. On the Menu bar, click **Reconfigure**.
4. In the Virtual Server and Pools section, from the **Should the BIG-IP system insert the X-Forwarded-For header?** question, select **Insert X-Forwarded-For HTTP header**.
5. Click **Finished**.

Deploying the Custom Logging role service

The first 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. If you receive this error, ensure that you are editing the log definition at the server level in IIS Manager.

The configuration is slightly different depending on which version of IIS you are running. Use the procedure applicable to your version of IIS.

To deploy the Custom Logging role service for IIS 7.0 and 7.5 (Windows Server 2008)

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 **Next**.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** button.

To deploy the Custom Logging role service for IIS 8.0 (Windows Server 2012)

1. From your Windows Server 2012 device, open Server Manager.
2. Click **Manage** and then **Add Roles and Features**.
3. Select Role-based or feature-based installation.
4. On the Roles screen, expand **Web Server (IIS)** and **Health and Diagnostics** and then check the box for **Custom Logging**.
5. Click **Next** and then on the Features screen, click **Next** again.
6. Click **Install**.
7. 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*

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*

The following procedure is the same for IIS versions 7.0, 7.5, and 8.0.

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

1. From your Windows Server device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server 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:
6. In the **Field ID** box, type **X-Forwarded-For**.
7. From the **Category** list, select **Default**.
8. From the **Source Type** list, select **Request Header**.
9. In the **Source Name** box, type **X-Forwarded-For**.
10. Click the **OK** button.
11. 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.
12. From the Actions pane on the right, click **Edit Log Definition**.
13. Click **Select Fields**, and then check the box for the X-Forwarded-For logging field.
14. Click the **OK** button.
15. From the Actions pane, click **Apply**.
16. Click **Return To Advanced Logging**.
17. In the Actions pane, click **Enable Advanced Logging**.
    Now, when you look at the Advanced Logging logs, the client IP address is included.

Glossary

application service

iApps Application Services use an *iApp Template* to guide users through configuring new BIG-IP® system configurations. An Application Service lets an authorized user easily and consistently deploy complex BIG-IP® system configurations just by completing the information required by the associated template. Every Application Service is attached to a specific configuration and cannot be copied the way that iApps templates can.

iApp Template

iApps templates create configuration-specific forms used by Application Services to guide authorized users through complex system configurations. The templates provide programmatic, visual layout and help information. Each new Application Service uses one of the templates to create a screen with fields and help that guide the user through the configuration process and creates the configuration when finished.

iApps templates allow users to customize by either modifying an existing template or creating one from scratch. Users can create scratch-built templates using either the iApps Templates screen or any text-editing software.

configuration utility

The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

custom profile

A custom *profile* is a profile that you create. A custom profile can inherit its default settings from a parent profile that you specify. See also parent profile.

health monitor

A health monitor checks a node to see if it is up and functioning for a given service. If the node fails the check, it is marked down. Different monitors exist for checking different services.

iRule

An iRule is a user-written script that controls the behavior of a connection passing through the BIG-IP system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence. You can attach iRules you created to your Microsoft SharePoint Application Service in the advanced configuration mode.

iSession

An iSession is an optimized connection between two BIG-IP systems.

iSession profile

An iSession profile defines the optimization parameters. WAN optimization requires an iSession profile, which specifies the optimization settings, such as compression and data deduplication. The iApp template uses the default isession profile.

load balancing method

A load balancing method or algorithm is a particular method of determining how to distribute connections across a *load balancing pool*. There are several different load balancing methods on the BIG-IP system. If you are working with servers that differ significantly in processing speed and memory, you might want to use a method such as Ratio or Weighted Least Connections.

Load balancing calculations can be localized to each pool (member-based calculation) or they may apply to all pools of which a server is a member (node-based calculation). For detailed information, see the product documentation.

See the table on the following page for a description of most load balancing methods.

Method	Description	When to use
Round Robin	Round Robin mode passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced.	Round Robin mode works well in most configurations, especially if the equipment that you are load balancing is roughly equal in processing speed and memory.
Ratio (member) **Ratio (node)**	The LTM distributes connections among pool members in a static rotation according to ratio weights you define. The number of connections each system receives over time is proportionate to the ratio weight you defined for each pool member. You set a ratio weight when you add each pool member in the iApp.	These are static load balancing methods, basing distribution on user-specified ratio weights that are proportional to the capacity of the servers.
Dynamic Ratio (member) **Dynamic Ratio (node)**	The Dynamic Ratio methods select a server based on various aspects of real-time server performance analysis. These methods are similar to the Ratio methods, except the ratio weights are system-generated, and the values of the ratio weights are not static. These methods are based on continuous monitoring of the servers, and the ratio weights are therefore continually changing.	The Dynamic Ratio methods are used specifically for load balancing traffic to RealNetworks® RealSystem® Server platforms, Windows® platforms equipped with Windows Management Instrumentation (WMI), or any server equipped with an SNMP agent such as the UC Davis SNMP agent or Windows 2000 Server SNMP agent. Note: To implement Dynamic Ratio load balancing, you must first install and configure the necessary server software for these systems, and then install the appropriate performance monitor.
Fastest (node) **Fastest (application)**	The Fastest load balancing mode load balances based upon the number of outstanding Layer 7 requests to a pool member and the number of open L4 connections.	The Fastest methods are useful in environments where nodes are distributed across separate logical networks.
Least Connections (member) **Least Connections (node)**	The Least Connections load balancing mode is a dynamic load balancing algorithm that distributes connections to the server that is currently managing the fewest open connections at the time the new connection request is received.	The Least Connections methods function best in environments where the servers have similar capabilities. Otherwise, some amount of latency can occur. If you have servers with varying capacities, consider using the Weighted Least Connections methods instead.
Weighted Least Connections (member) **Weighted Least Connections (node)**	Specifies that the system passes a new connection to the pool member that is handling the lowest percentage of the specified maximum number of concurrent connections allowed. This mode requires that you specify a value for the connection-limit option for all members of the pool.	This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits.
Observed (member) **Observed (node)**	With the Observed methods, nodes are ranked based on the number of connections. The Observed methods track the number of Layer 4 connections to each node over time and create a ratio for load balancing	The need for the Observed methods is rare, and they are not recommended for large pools.
Predictive (member) **Predictive (node)**	The Predictive methods use the ranking methods used by the Observed methods. However, with the Predictive methods, LTM analyzes the trend of the ranking over time, determining whether a nodes performance is currently improving or declining. The servers with performance rankings that are currently improving receive a higher proportion of the connections.	The need for the Predictive methods is rare, and they are not recommended for large pools.
Least Sessions	The Least Sessions method selects the server that currently has the least number of entries in the persistence table. Use of this load balancing method requires that the virtual server reference a type of profile that tracks persistence connections, such as the Source Address Affinity or Universal profile type. Note: The Least Sessions methods are incompatible with cookie persistence.	The Least Sessions method works best in environments where the servers or other equipment that you are load balancing have similar capabilities.

load balancing pool

A load balancing pool is a logical set of devices, such as web servers, that you group together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, Local Traffic Manager sends the request to any of the servers that are members of that pool. This helps to efficiently distribute the load on your server resources.

local endpoint

The local endpoint is the BIG-IP system on which you are currently working. The systems must be set up symmetrically, so that a local endpoint connects to one or more remote endpoints.

network virtual server

A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0, such as 192.168.1.0). This allows you to direct client traffic based on a range of destination IP addresses.

profile

Profiles are a configuration tool that you can use to affect the behavior of certain types of network traffic. More specifically, a profile is an object that contains settings with values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Profiles also provide a way for you to enable connection and session persistence, and to manage client application authentication.

self IP address

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access the internal and external VLANs.

SNAT

A SNAT (Secure Network Address Translation) is a feature that defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNAT pool

A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses.

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 port. This is the address clients use to connect to the SharePoint servers (or a FQDN resolves to this address). The BIG-IP intercepts the client request, and then directs the traffic according to your configuration instructions.

VLAN

A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

Document Revision History

Version	Description	Date
RC-1	New Deployment Guide for the f5.microsoft_sharepoint_2010_2013.v1.1.0rc1 version of the iApp template available on DevCentral which includes BIG-IP AFM configuration and an additional logging profile option in the BIG-IP ASM section.	04-23-2014
RC-1a	Added *Supporting Host-Named Site Collections in SharePoint Server 2010 and 2013 (optional) on page 34.* Added a new troubleshooting entry on page 40 with a link to a Microsoft hotfix for users experiencing issues opening SharePoint documents in Windows Explorer or editing SharePoint documents in Microsoft applications.	05-14-2014
RC-1b	Added the new section *Modifying the HTTP compression profile if using a previous version of the template on page 35*, with a required change to the HTTP Compression profile. Added the same change to the manual configuration table.	05-23-2014
RC-1c	Further modified the section *Modifying the HTTP compression profile if using a previous version of the template on page 35*, with two missing entries for the Content Include list. Added the same change to the manual configuration table.	05-28-2014
RC-1d	Added a new troubleshooting entry on page 40 for client connections that are unresponsive or seem to hang when using the OneConnect feature.	06-20-2014
1.0	- Updated the guide for the fully supported iApp f5.microsoft_sharepoint_2010_2013.v1.1.0 available on downloads.f5.com. - Renamed the section *Modifying the configuration produced by the iApp template* which described an HTTP compression profile modification, to *Modifying the HTTP compression profile if using a previous version of the template*, as it has been fixed in version 1.1.0 of the template.	07-16-2014
1.1	- Added support for BIG-IP version 11.6. - Added the new section *Manually configuring the BIG-IP Advanced Firewall Module to secure your SharePoint deployment on page 50*.	08-25-2014
1.2	Added the new section *Modifying the iApp configuration if you configured the iApp to create a new LDAP monitor for the AD pool on page 32*.	09-30-2014
1.3	- Added the new entry to the troubleshooting section on page 41 if users are having issues with APM single sign-on. - Added the new section *Optional: Monitoring SharePoint Web Applications Configured for AD FS as a Trusted Identity Provider on page 30*. Added a reference to this section in the manual configuration table.	10-09-2014
1.4	- Added a new entry to the troubleshooting section on page 41 with a required modification to the configuration produced by the iApp template if using BIG-IP AFM and the IP Intelligence database to log or restrict traffic with low reputation scores.	11-04-2014
1.5	Added a link to the Release Candidate deployment guide on page 1.	12-16-2014
1.6	Added the new section *Configuring BIG-IP LTM/APM to support NTLMv2-only deployments (optional) on page 36*.	04-23-2015

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