Deploying F5 with Microsoft Active Directory Federation Services

This F5 deployment guide provides detailed information on how to deploy Microsoft Active Directory Federation Services (AD FS) with F5's BIG-IP LTM and APM modules. The BIG-IP LTM provides high availability, performance, and scalability for both AD FS and AD FS Proxy servers. Additionally, you can choose to deploy the Access Policy Manager to secure AD FS traffic without the need for AD FS Proxy servers.

For more information on Microsoft AD FS, see *http://social.technet.microsoft.com/wiki/contents/articles/2735.ad-fs-content-map.aspx*
For more information on the BIG-IP system, see *http://www.f5.com/products/bigip/*

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

Products and versions tested

Product	Versions
BIG-IP LTM and APM	Microsoft AD FS **2.0**: BIG-IP v11.0 - 11.6 Microsoft AD FS **3.0**: BIG-IP v11.4.1 - 11.6
Microsoft Active Directory Federation Services	2.0, 3.0
Deployment guide version	1.8 (see *Document Revision History on page 12*)

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

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

Microsoft Partner Network

Contents

Prerequisites and configuration notes 3

Configuration example 3

Configuring the BIG-IP LTM for Microsoft AD FS 7

Configuring the BIG-IP LTM for load balancing AD FS or AD FS proxy servers 7

Configuring the BIG-IP Access Policy Manager for AD FS 9

Appendix A: Configuring DNS and NTP on the BIG-IP system 12

Configuring the DNS settings 12

Configuring the NTP settings 12

Document Revision History

Prerequisites and configuration notes

The following are general prerequisites for this deployment; each section contains specific prerequisites:

- All of the configuration procedures in this document are performed on F5 devices. For information on how to deploy or configure AD FS, consult the appropriate Microsoft documentation.
- You must be on BIG-IP LTM version 11.0 or later. We recommend version 11.4 or later.
- You must have already installed the F5 device(s) in your network and performed the initial configuration tasks, such as creating Self IP addresses and VLANs. For more information, refer to the appropriate BIG-IP LTM manual, available at *http://support.f5.com/kb/en-us.html*.
- You must have correctly installed and configured AD FS 2.0 or 3.0 in your environment, and confirmed that you have enabled a service endpoint, such as *https://localhost/adfs/fs/federationserverservice.asmx* from the AD FS server(s), and can browse to it.
- When deploying APM in front of AD FS, the AD FS Global Primary Authentication Policy for the Intranet zone should be set to **Windows Authentication**.
- If you are forwarding traffic from AD FS Proxy servers to a virtual server load balancing AD FS servers, and using the iApp template, you must select **Encrypted traffic is forwarded without decryption (SSL pass-through)** in response to the question *How should the BIG-IP system handle SSL traffic?* Due to certificate authentication requirements between the AD FS proxy servers and AD FS servers, terminating and re-encrypting SSL is not supported in this configuration.

Configuration example

There are three ways you can configure the BIG-IP system for Microsoft AD FS deployments: using the BIG-IP LTM to load balance AD FS servers, using the BIG-IP LTM to load balance AD FS proxy servers, and using the BIG-IP APM to secure AD FS traffic without the need for proxy servers.

Load balancing AD FS with the BIG-IP system

In this scenario, the F5 LTM module optimizes and load balances requests to an internal AD FS server farm.

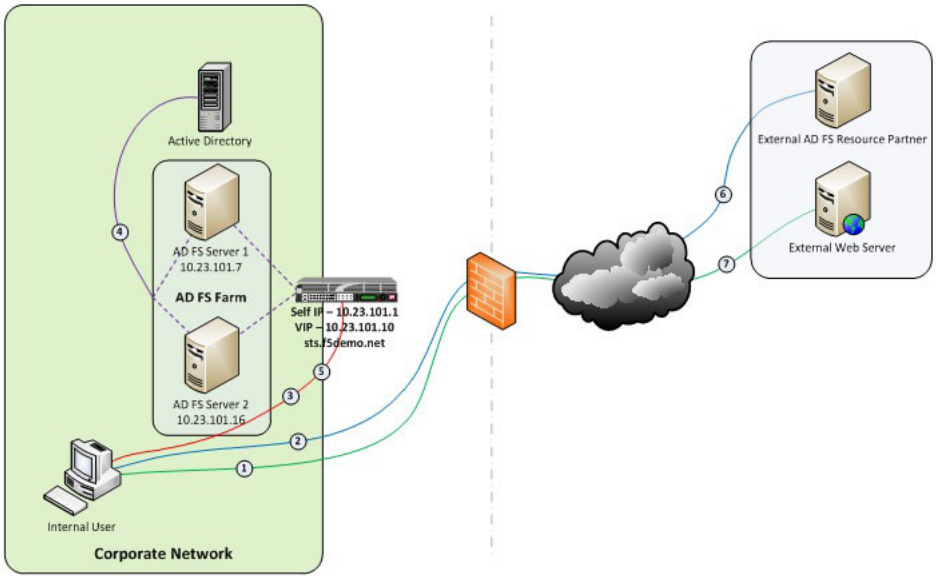

Figure 1: *Logical configuration diagram: Load Balancing AD FS*

The following is the traffic flow for this scenario.

1. A client attempts to access the AD FS-enabled external resource.
2. The client is redirected to the resource's applicable federation service.
3. The client is redirected to its organization's internal federation service, (assuming the resource's federation service is configured as trusted partner).

4. The AD FS server authenticates the client to Active Directory.
5. The AD FS server provides the client with an authorization cookie containing the signed security token and set of claims for the resource partner.
6. The client connects to the resource partner federation service where the token and claims are verified. If appropriate, the resource partner provides the client with a new security token.
7. The client presents the new authorization cookie with included security token to the resource for access.

Load balancing AD FS proxy servers with the BIG-IP system

In this scenario, the F5 LTM module optimizes and load balances requests to an external AD FS Proxy server farm.

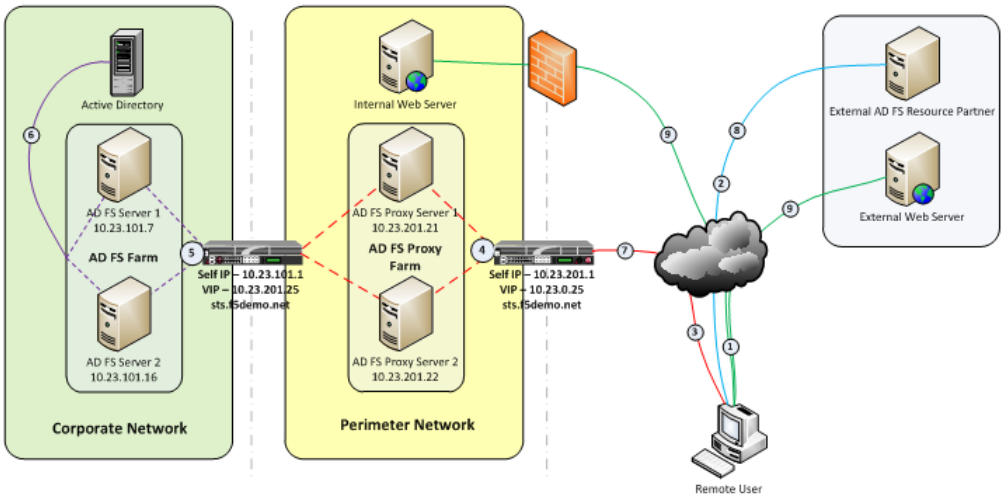

Figure 2: *Logical configuration diagram: Load Balancing AD FS proxy servers*

The following is the traffic flow for this scenario.

1. A client attempts to access the AD FS-enabled internal or external resource.
2. The client is redirected to the resource's applicable federation service.
3. The client is redirected to its organization's internal federation service, (assuming the resource's federation service is configured as trusted partner).
4. The AD FS proxy server presents the client with a customizable sign-on page.
5. The AD FS proxy presents the end-user credentials to the AD FS server for authentication.
6. The AD FS server authenticates the client to Active Directory.
7. The AD FS server provides the client, (via the AD FS proxy server) with an authorization cookie containing the signed security token and set of claims for the resource partner.
8. The client connects to the resource partner federation service where the token and claims are verified. If appropriate, the resource partner provides the client with a new security token.
9. The client presents the new authorization cookie with included security token to the resource for access.

Securing AD FS with the BIG-IP APM

In this scenario, the F5 APM module secures, optimizes, and load balances requests to an internal or external AD FS server farm, eliminating the need to deploy AD FS Proxy servers in a perimeter network.

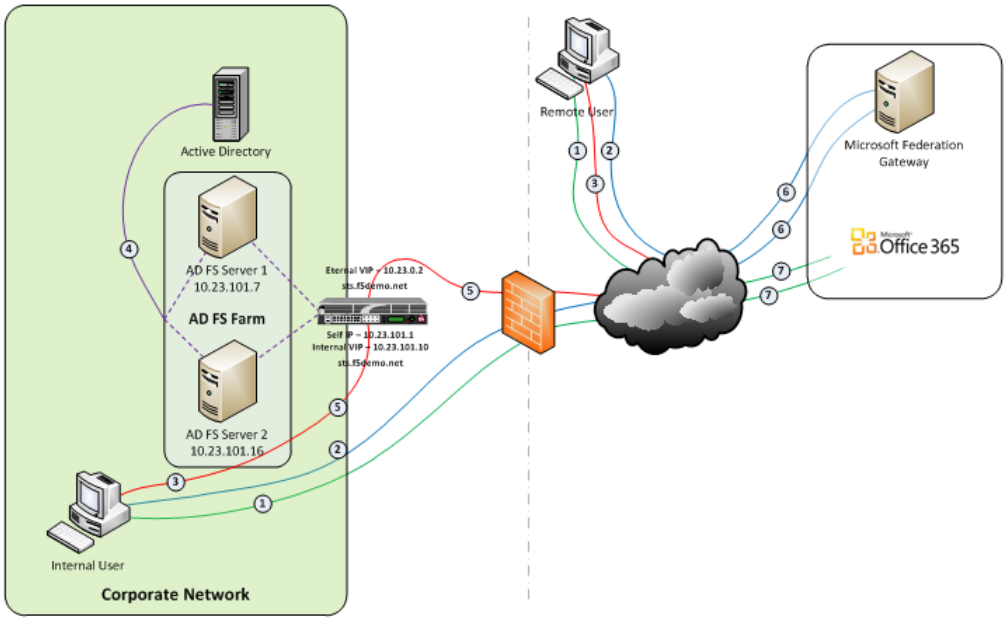

Figure 3: *Logical configuration diagram: Using BIG-IP APM*

The following is the traffic flow for this scenario.

1. Both clients attempt to access the Office 365 resource;
2. Both clients are redirected to the resource's applicable federation service, (Note: This step may be skipped with active clients such as Microsoft Outlook);
3. Both clients are redirected to their organization's internal federation service;
4. The AD FS server authenticates the client to Active Directory;
5. Internal clients are load balanced directly to an AD FS server farm member; and
6. External clients are:
7. Pre-authenticated to Active Directory via APM's customizable sign-on page;
8. Authenticated users are directed to an AD FS server farm member.
9. The AD FS server provides the client with an authorization cookie containing the signed security token and set of claims for the resource partner;
10. The client connects to the Microsoft Federation Gateway where the token and claims are verified. The Microsoft Federation Gateway provides the client with a new service token;
11. The client presents the new cookie with included service token to the Office 365 resource for access.

Configuring the BIG-IP LTM for Microsoft AD FS

The following tables contain a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment scenario. Unless otherwise specified, settings not mentioned in the tables can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Configuring the BIG-IP LTM for load balancing AD FS or AD FS proxy servers

Health Monitors (*Main tab > Local Traffic > Monitors*)		
If using AD FS 2.0, choose one of the first two monitors. If using AD FS 3.0, you must use the External monitor.		
AD FS 2.0: Monitor if load balancing AD FS servers		
Name	Type a unique name	
Type	**HTTPS**	
Interval	**30** (recommended)	
Timeout	**91** (recommended)	
Send String[1]	**GET /adfs/fs/federationserverservice.asmx HTTP/1.1\r\nHost: sts1.example.com\r\nConnection: Close\r\n**	
Receive String	**200 OK**	
AD FS 2.0: Monitor if load balancing AD FS Proxy servers		
Name	Type a unique name	
Type	**HTTPS**	
Interval	**30** (recommended)	
Timeout	**91** (recommended)	
Send String	**GET /\r\n** (the default)	
AD FS 3.0: External Monitor		
Name	Type a unique name	
Type	**External**	
Interval	**30** (recommended)	
External Program	See *Importing the script file for AD FS 3.0 health monitor on page 7*	
Variables	**Name** / **Value** **HOST** — Type the FQDN clients will use to access the AD FS deployment, such as sts.example.com. **URI** — Type the URI of the resource you want to monitor, such as /adfs/fs/federationserverservice.asmx. **RECV** — Type the expected response, such as 200 OK.	
Pools (*Main tab > Local Traffic > Pools*)		
Name	Type a unique name	
Health Monitor	Select the monitor you created above	
Load Balancing Method	**Least Connections (Member)**	
Address	Type the IP Address of an AD FS server or AD FS Proxy Server	
Service Port	**443** Click **Add** to repeat Address and Port for all nodes	
Profiles (*Main tab > Local Traffic > Profiles*)		
HTTP *(Profiles > Services)*	Name Parent Profile	Type a unique name **http**
TCP WAN *(Profiles > Protocol)*	Name Parent Profile	Type a unique name **tcp-wan-optimized**
TCP LAN *(Profiles > Protocol)*	Name Parent Profile	Type a unique name **tcp-lan-optimized**
Client SSL *(Profiles > SSL)*	Name Parent Profile Certificate and Key	Type a unique name **clientssl** Select the Certificate and Key you imported from the associated list
Server SSL *(Profiles > Other)*	Name Parent Profile Server Name <only 3.0>	Type a unique name **serverssl** Type the FQDN clients will use to access the AD FS deployment (If using AD FS 3.0, this must be the same value as the monitor HOST variable)

[1] *Replace red text with your FQDN*

Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Type	**Standard**
Destination Address	Type the IP address for this virtual server
Service Port	**443**
VLAN and Tunnel Traffic	If applicable, select specific VLANs and Tunnels on which to allow or deny traffic.
Protocol Profile (client)	Select the WAN optimized TCP profile you created above
Protocol Profile (server)	Select the LAN optimized TCP profile you created above
HTTP Profile	Select the HTTP profile you created
SSL Profile (Client)	Select the Client SSL profile you created above
SSL Profile (Server)	If you created a Server SSL profile, select it from the list
SNAT Pool[2]	**Auto Map**[2]
Default Pool	Select the pool you created above

[2] *In version 11.3 and later, this field is* ***Source Address Translation****. If you want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation specific information.*

Note: *Your DNS A record for the AD FS endpoint must reference the AD FS or AD FS Proxy BIG-IP virtual server. If you are deploying the BIG-IP system in front of both AD FS and AD FS Proxy servers, you must use a host file entry on the AD FS Proxy servers that resolves the AD FS endpoint FQDN to the IP address of the AD FS BIG-IP virtual server.*

Importing the script file for AD FS 3.0 health monitor

Before you can create the advanced monitors you must download and import the applicable monitor file onto the BIG-IP system.

Note: *If you are using a redundant BIG-IP system, you need to make sure any modifications to the script EAVs are manually copied between BIG-IP LTMs, and given the required permissions when configuration is synchronized.*

To download and install the script

1. Download the script: *http://www.f5.com/pdf/deployment-guides/sni-eav.zip*
2. Extract the appropriate file(s) to a location accessible by the BIG-IP system.
3. From the Main tab of the BIG-IP Configuration utility, expand **System**, and then click **File Management**.
4. On the Menu bar, click **External Monitor Program File List**.
5. Click the **Import** button.
6. In the **File Name** row, click **Browse**, and then locate the appropriate file.
7. In the **Name** box, type a name for the file related to the script you are using.
8. Click the **Import** button.

Now when you create the advanced monitors, you can select the name of the file you imported from the **External Program** list.

Configuring the BIG-IP Access Policy Manager for AD FS

In this section, we provide guidance on configuring the BIG-IP Access Policy Manager (APM) to help protect your Microsoft AD FS deployment without the need for AD FS proxy servers. This part of the configuration is in addition to the BIG-IP LTM configuration described previously. If you have not yet configured the BIG-IP LTM, we recommend you return to *Configuring the BIG-IP LTM for Microsoft AD FS on page 6* and configure the LTM first.

Use the following table to manually configure the BIG-IP APM. 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 instructions on configuring individual objects, see the online help.

Important *As stated in the prerequisites, when deploying APM in front of AD FS, the Intranet Global Primary Authentication Policy should be set to* ***Windows Authentication****.*

DNS and NTP	
DNS and NTP	See *Appendix A: Configuring DNS and NTP on the BIG-IP system on page 11* for instructions.
AAA Server (*Main tab-->Access Policy-->AAA Servers)*	
Name	Type a unique name
Type	**Active Directory**
Domain Name	Type the FQDN of Active Directory domain where users will authenticate (i.e. “example.com”)
Server Connection	**Use Pool**
Domain Controller Pool Name	Type a name for this pool of Active Directory servers
Domain Controllers	Type the IP address and the FQDN for each Domain Controller you want to add and then click Add.
Server Pool Monitor	**gateway_icmp** (or a custom monitor if you created one).
Admin Name/Password	If required, type the Admin name and Password
SSO Configuration (*Main tab > Access Policy > SSO Configuration*)	
Name	Type a unique name
SSO Method	**NTLMV1**
Username Conversion	**Enable**
NTLM Domain	Type the NTLM Domain name
iRules (*Main tab > Local Traffic > iRules*)	
Optional: *This optional iRule disables APM for MS Federation Gateway. See Optional iRule to disable APM for MS Federation Gateway on page 9*	
Name	Type a unique name
Definition	Use the Definition in *Optional iRule to disable APM for MS Federation Gateway on page 9*
Connectivity Profile (*Main tab > Access Policy > Secure Connectivity*)	
Name	Type a unique name
Parent Profile	**connectivity**
Access Profile (*Access Policy-->Access Profiles*)	
Name	Type a unique name
Profile Type	**LTM-APM** (BIG-IP v11.5 and later only)
Inactivity Timeout	We recommend a short time period here, such as 10 seconds.
Domain Cookie	If deploying for AD FS only, we recommend leaving this field blank. If you are applying this profile to multiple virtual servers, type the parent domain.
Primary Authentication URI	(**Optional**; for Multiple Domains mode only. See the Access Profile help or documentation for information) Type the URL of the AD FS service, such as https://sts1.example.com. Include additional domains if necessary.
SSO Configuration	Select the SSO configuration you created.
Languages	Move the appropriate language(s) to the **Accepted** box.
Edit the Access Policy	
Edit the Access Profile you just created using the Visual Policy Editor. Continue now with Editing the Access Policy.	
Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Open the BIG-IP LTM virtual server you created by clicking **Local Traffic > Virtual Servers >** *name you gave the LTM virtual server. After editing the Access Policy, add the following BIG-IP APM objects you just created.*	
Access Profile	Select the Access profile you created
Connectivity Profile	Select the Connectivity profile you created
iRules	If you created the iRule to disable APM for MS Federation Gateway, select the iRule and Enable it.

Editing the Access Policy

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

To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click the **Add Item** button.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click **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. You have to apply an access policy before it takes effect.
14. The VPE should look similar to the following example. Click the **Close** button on the upper right to close the VPE.

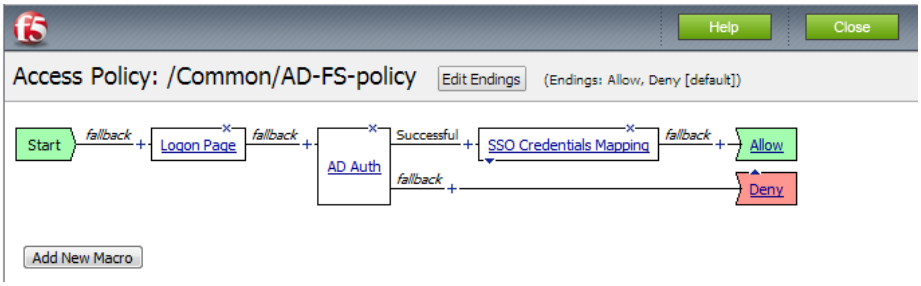

Figure 4: *Logical configuration diagram: Using BIG-IP APM*

Optional iRule to disable APM for MS Federation Gateway

For clients that use the Active WS-Trust protocol, an iRule is required to disable BIG-IP APM for requests to the MS Federation Gateway. Attach the following iRule to the previously created APM-enabled BIG-IP virtual server to proxy passive protocol requests from
browser-based clients, and bypass the BIG-IP APM for requests from clients such as Outlook and Lync.

To create the iRule, go to **Local Traffic > iRules** and then click Create. Use the following code in the Definition section.

```
when HTTP_REQUEST {
   # For external Lync client access all external requests to the
   # /trust/mex URL must be routed to /trust/proxymex. Analyze and modify the URI
   # where appropriate
   HTTP::uri [string map {/trust/mex /trust/proxymex} [HTTP::uri]]

   # Analyze the HTTP request and disable access policy enforcement WS-Trust calls
   if {[HTTP::uri] contains "/adfs/services/trust"} {
         ACCESS::disable
   }

   # OPTIONAL ---- To allow publishing of the federation service metadata
   if {[HTTP::uri] ends_with "FederationMetadata/2007-06/FederationMetadata.xml"} {
         ACCESS::disable
   }
}
```

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

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

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.

Document Revision History

Version	Description	Date
1.0	New Version	03-13-2014
1.1	- Added a row to the BIG-IP APM configuration table for the Access profile on page 8 concerning the optional ability to configure the Access Profile to apply the SSO configuration across multiple authentication domains. - Added support for BIG-IP version 11.5.1	05-23-2014
1.2	- Updated the guide to include configuration for AD FS 3.0. - Modified the APM configuration table to remove LTM-specific objects. Virtual server configuration section of the table is now an update to the existing LTM virtual server to include the APM objects. - Added support for BIG-IP version 11.6	10-09-2014
1.3	- Modified the virtual server **Type** setting from **Performance L4** to **Standard**. - Removed the Rewrite Redirect setting from the HTTP profile.	12-19-2014
1.4	- Updated the External monitor script file referenced in *Importing the script file for AD FS 3.0 health monitor on page 7.* Only the linked script file was changed, there were no changes to the content of this guide.	02-13-2015
1.5	- Updated the External monitor script file referenced in *Importing the script file for AD FS 3.0 health monitor on page 7.* Only the linked script file was changed, there were no changes to the content of this guide.	03-19-2015
1.6	- Updated the guidance in the BIG-IP APM manual configuration table on *page 8* for the Access Policy > Domain Cookie value, depending on whether APM is deployed for AD FS only or if applying the profile to multiple virtual servers	04-09-2015
1.7	- Updated the External monitor script file referenced in *Importing the script file for AD FS 3.0 health monitor on page 7.* Only the linked script file was changed, there were no changes to the content of this guide.	06-08-2015
1.8	- Added a bullet item to *Prerequisites and configuration notes on page 3* concerning forwarding traffic from AD FS proxy servers to a virtual server load balancing AD FS servers. - Updated the format of this guide.	06-10-2015

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